NHS
Counter Fraud Authority

Strategic Intelligence Assessment 2025

Covering 2024 - 2025

Working together to find, report and stop NHS fraud

Contents

Foreword 3

Executive summary 5

Introduction 7

How do we calculate fraud vulnerability? 11

Reporting trends 13

Cyber-facilitated fraud 16

Procurement and commissioning of services fraud 18

Patient exemption fraud 21

Data manipulation fraud 23

Community pharmaceutical contractor fraud 26

General Practice (GP) contractor fraud 30

Optical contractor fraud 32

Dental contractor fraud 34

NHS staff fraud 36

Fraudulent access to NHS care from overseas visitors 39

Reciprocal healthcare fraud 42

Foreword

Safeguarding our National Health Service's financial resources is of critical importance. This year's Strategic Intelligence Assessment reveals that while £1.346 billion of NHS funding remains vulnerable to fraud, bribery, and corruption, this represents a smaller percentage of our overall budget compared to previous years – a testament to our strengthening counter fraud approach across the health sector. However, £1.346 billion could supply the NHS with so much – including doctors, nurses, ambulances and equipment to enable the NHS to move from analogue to digital, hospital to community and sickness to prevention – helping save lives and making a difference to people's health.

The healthcare landscape continues to evolve rapidly. There will be structural changes as NHS England (NHSE) is merged with the Department of Health and Social Care (DHSC), the 10 Year Health Plan is introduced and Integrated Care Systems consolidate. Against this backdrop of transformation, our mission to protect NHS resources is vital. This assessment, which is unique to us, ensures that stakeholders are appropriately informed and equipped to act to find and prevent fraud in an increasingly complex environment.

In addition to providing an estimate on the amount of the NHS funding vulnerable to fraud, bribery and corruption. The SIA also provides an assessment of threats, vulnerabilities and enablers for prevention and enforcement activity. The intelligence gathered in this assessment will drive our strategic and tactical response in the coming year, informing targeted interventions and collaborative efforts across the system. Our intelligence-led approach, guided by the National Intelligence Model, ensures we remain agile in addressing both current and emerging threats.

I am particularly encouraged by the continued success of Real-Time Exemption Checking (RTEC). These technological solutions, alongside enhanced reporting mechanisms and cross-sector collaboration, demonstrate our commitment to innovation in counter fraud.

Over the last year we, in partnership with our stakeholders, targeted procurement and commissioning fraud, which we estimate to have the highest amount of fraud vulnerability of the thematic areas described in the report. This work is complete with over 390 Local Proactive Exercises (LPEs) undertaken in England and has resulted in a significant number of changes in NHS policy and processes to close system weaknesses. Over the next year we will focus on staff fraud and have established a working group to develop our response.

Project Athena, which was launched at the beginning of 2024, is now embedded. We have established a team of data scientists, analysts and engineers to deploy artificial intelligence and machine learning, enabling us to analyse large amounts of data to detect fraudulent activity. We have also gained access to several key

data sources, such as Companies House information and Civil Registrations of Death, which provide insights that support efficient and effective investigations. We will continue to build on this progress over the coming year, which will in turn inform our SIA, ensure a strong counter fraud response and support delivery of the 10 Year Health Plan to create an NHS fit for the future.

The SIA requires extensive collaboration, analysis, and effort from partners across the health system and colleagues within the NHSCFA. I extend my sincere thanks to everyone involved in its production, and I look forward to using this document as we work together to counter fraud over the coming year.

Alex Rothwell
Chief Executive Officer

Executive summary

The NHSCFA estimates that £1.346 billion of NHS funding is vulnerable to loss through fraud, bribery, and corruption in England[a]. This equates to 0.72% of the NHS budget vulnerable to fraud for 2024 - 2025 and is therefore a percentage decrease when compared with the NHS budget for 2023 - 2024. Although the allocated budget for the NHS in England has increased by over 9% to £186.838[b] billion for 2024 – 2025.

Reports received by the NHSCFA have increased to 6,462 during 2024 – 2025. The table below breaks down the current reporting figures by thematic area and displays the financial vulnerability estimates for 2024 - 2025 compared with 2023 - 2024.

Strategic priority area	2024 - 2025 financial vulnerability estimate[c]	2023 - 2024 financial vulnerability estimate	Difference (£m)	2024 -2025 reports received by the NHSCFA
Procurement and commissioning fraud	£392.5m	£388.3m	+ £4.2m	537
Patient exemption fraud	£230.2m	£240.2m	- £10m	1,238
Data manipulation fraud	£189.1m	£165.1m	+ £23m	25
Community pharmaceutical contractor fraud	£135.2m	£130.2m	+ £5m	238
GP contractor fraud	£116.7m	£110.1m	+ £6.6m	233
Optical contractor fraud	£90.7m	£94m	- £3.4m	41
Dental contractor fraud	£57.6m	£58.6m	- £1m	74
NHS staff fraud	£27.8m	£31.9m	- £4m	3,211
Fraudulent access to NHS care from overseas visitors	£98.1m	£86.5m	+ £11.6m	387
Reciprocal healthcare fraud	£0.8m	£0.4m	+ £0.4m	6
Strategic oversight area				
NHS Bursary fraud	£3.8m	£3.2m	+ £0.6m	23
NHS Pension fraud	£4.1m	£7m	- £2.9m	31
Total	**£1.346bn**	**£1.316bn**	**£30.9m**	**6,044[d]**

[a] This is not a figure of actual financial loss from fraud, but an estimate of the amount of funding vulnerable to the risk of loss.
[b] Total NHS revenue department expenditure limit (RDEL) as per financial directions.
[c] Financial vulnerability estimates run a year in arrears to reporting data, therefore this assessment will include 2023 – 2024 financial data and 2024 – 2025 reporting data.
[d] There are an additional 418 reports which did not align to a thematic area; therefore, the overall total is 6,462.

Reporting received by the NHSCFA reporting has increased by 1.5% when compared with 2023 – 2024, which is in line with fraud in England and Wales increasing by 7% in December 2024 when compared to December 2023.

Approximately 83.2% of reports this year relate to NHS staff fraud, patient exemption fraud, procurement and commissioning fraud, and fraudulent access to NHS care from overseas visitors.

The Procurement Act 2023 now allows all suppliers to compete for public contracts through a centralised application and tender process. These more flexible frameworks help suppliers and procurers work more collaboratively and reduce costs. This current reporting period has seen the first full year of the Provider Selection Regime (PSR). PSR is designed to introduce more flexibility, enable stable collaboration and remove levels of competitive tendering for the best interests of patient and service users. Yet, a vulnerability has arisen as PSR enables those in decision-makers to avoid competitive tendering by arguing that a change of current supplier is not required, or a supplier for a new contract has already been identified.

Following a proactive prevention exercise in 2022-2023 there has been reduced reporting and recorded financial loss relating to the threat of payment diversion fraud however this methodology remains prominent with instances of cyber enabled fraud by criminals to divert genuine payments or falsify payments observed. The reductions suggest that criminals are finding it harder to infiltrate NHS counter measures.

An emerging trend has been identified where individuals are impersonating NHS staff to perform NHS bank shifts. These shifts are reported to be carried out by another person using a genuine staff members ID, whilst they perform their substantive role.

A new modus operandi (MO) has arisen where the journey of accessing the NHS without charge when not entitled was reported to have been posted on a social media platform. Thus, publicising fraudulent access to the NHS for non-ordinary residents and potentially influencing those who aren't eligible.

The NHS and other healthcare agencies are targets for cyber criminals with health data having the potential to be more valuable than banking data.

The NHSCFA is intelligence led and looks to the National Intelligence Model for strategic direction. This combined with the support of our four strategic pillars drives forward counter fraud activity to protect funds meant for patient care.

Over the past year we have continued to expand and improve our working relationships within the counter- fraud community, both newly established and continuous stakeholder relations have not only increased confidence in our analysis, whilst maintaining its reliability and accuracy. Stakeholders should note the contents of this report and initiate action to develop appropriate counter-fraud measures, for example mitigating the detailed enablers.

Introduction

The Strategic Intelligence Assessment is produced to establish fraud threats and estimate the amount of funding for the NHS in England vulnerable to fraud, bribery and corruption annually on behalf of the Department of Health and Social Care (DHSC). This informs the NHSCFA and its stakeholders of the priorities for the year ahead by capturing established, emerging, and potential future threats. The SIA has, and will continue to, ensure a coordinated response to fraud.

Since 2016–2017, the NHSCFA has continued to monitor and document the ongoing fraud threat facing the NHS in England. The SIA remains a consistent and reliable source for the fraud community to draw upon. Because fraudsters are quick to adapt to their current climate, the NHSCFA's analysis is crucial to identifying the threats and intelligence gaps within an ever-evolving landscape. Allowing a coordinated response to fraud across the health sector and the maintenance of checks and balances that act as an effective deterrent.

The financial vulnerability is an estimate of how much NHS funding is exposed to the risk of loss from fraud. The current figure equates to 0.72% of the NHS budget for 2024 - 2025 and is a percentage decrease when compared with the previous budget. Although we have seen a financial vulnerability increase of £30.9 million (2.4%) when compared with the previous SIA, the allocated budget for the NHS in England has increased by over 9% to £186.838[e] billion for 2024 – 2025. Therefore, it is likely that there is a correlation between the increase in budgets and an increase in the amount vulnerable to fraud. Although the overall financial vulnerability has increased, the decrease in the percentage of the budget vulnerable to fraud showcases an effective counter fraud approach across the health sector contrary to fraud increasing in England and Wales by 33% since 2017[f]. The financial vulnerability data runs a year in arrears to reporting data therefore, this assessment will include 2023 – 2024 financial data and 2024 – 2025 reporting data.

Across 2024 – 2025 there have been increases within procurement in clinical expenditure, driven by inflation and changes in drugs and devices used. There has also been an increase in the number of prescription items dispensed, alongside a cost per item increase. Dentists are offered incentives with the aim of creating more than 2.5 million NHS appointments, with a minimum Unit of Dental Activity (UDA) rate being implemented. This reporting period also contains the second year of a £645 million investment for an expansion in primary care access in community pharmacy, including the Pharmacy First initiative. Additionally, member state claims issued against the UK, as well as the cost of a European Health Insurance Card (EHIC)/Global Health Insurance Card (GHIC) application increased. Furthermore, funding allocated to Integrated Care Boards (ICBs) has increased in comparison to the previous year, but inflation has reportedly still eroded the financial allocations received by trusts potentially incentivising fraudulent activity to plug the gap.

[e] Total NHS revenue department expenditure limit (RDEL) as per financial directions
[f] Between year-end March 2017 December 2024 - ONS

Reporting received by the NHSCFA has increased by 95 reports to 6,462 during 2024 – 2025. It is possible that with individuals reporting they are dissatisfied with the NHS, staff and patients may look to reporting fraud to improve circumstances. Furthermore, the cost-of-living crisis and global landscape can influence reporting patterns.

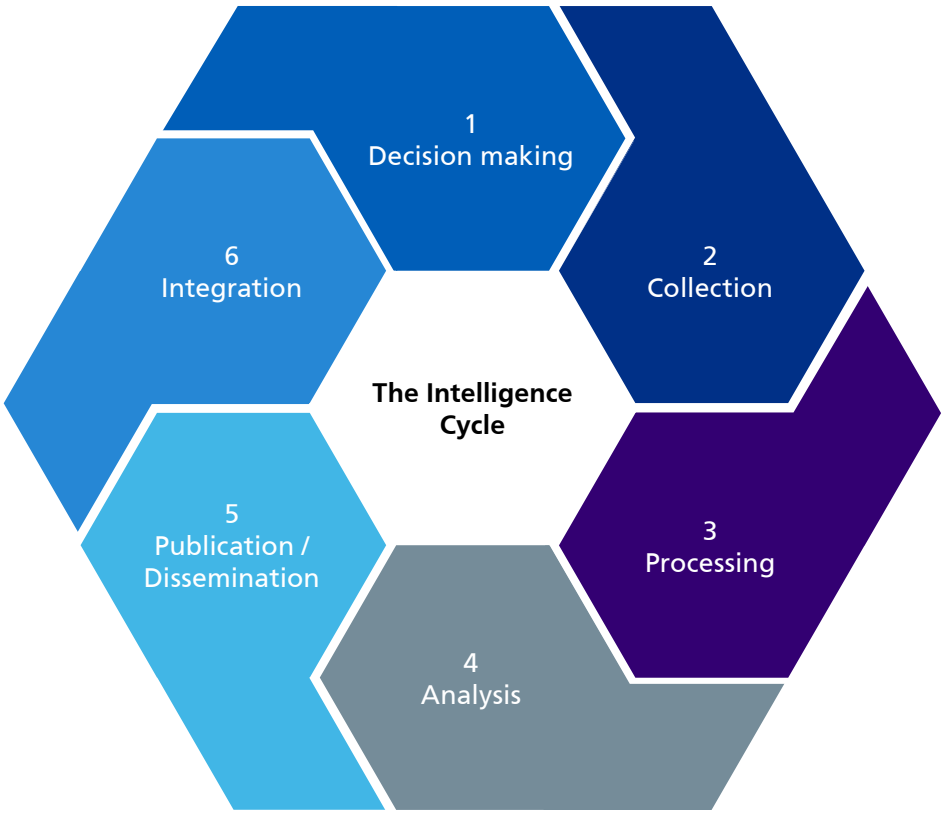
The NHS is exposed to increasing pressures and an ever-changing landscape both domestically and globally. Winter 2024 - 2025 A&E attendances were the highest on record, described as in line with a growing and aging population, although a disproportionate number of operational problems occurred. Bed occupancy has risen over the last 15 years and 11% of patients waited 12 hours before being admitted into hospital in January 2025. Although staff vacancies across the NHS were at 7.2% and overall sickness absence rates at 5.7%, a staff survey reported that one-third stated there were enough staff to perform their jobs properly.

In March 2025, the government announced that NHS England will merge with the DHSC, whilst Integrated Care Boards (ICBs) will be required to halve their costs, and the new NHS 10-Year Health Plan aims to result in transformation across healthcare. Additionally, the UK was impacted by the baseline tariff[g] as part of the reciprocal tariffs introduced by the United States of America which could impact on healthcare costs. Change therefore continues to alter on the NHSCFA's knowledge base, and we are continuously working to re-establish expertise and close intelligence gaps.

The NHSCFA's 2025-2026 Business Plan details how we will protect the NHS from fraud, bribery and corruption through leading the NHS response, empowering others and being experts in our field, whilst also putting the interests of the NHS and its patients first. This is possible because the NHSCFA is an intelligence led authority which looks to the National Intelligence Model (NIM) for strategic direction, and with the support of our four strategic pillars[h] we continue to improve our alignment to this model and support counter fraud activity against the backdrop of an ever-evolving landscape.

The NIM helps us to identify medium to long term priorities and prioritise the allocation of resources based on demand. The NHSCFA therefore follows the intelligence cycle to formulate these strategic plans, and the Strategic Intelligence Assessment is a key part of this. The DHSC-NHSCFA framework agreement and cycle require the production of a strategic assessment annually which identifies the threats and our understanding of them, as well as intelligence gaps and emerging trends to inform the NHSCFA and its stakeholders of the priorities for the year ahead. Therefore, the decision-making stage of the intelligence cycle determines what information will be collected based on intelligence from the previous cycle.

[g] Other than with automobiles
[h] Understand, Prevent, Respond and Assure



The collection stage involves gathering data through various methods to meet intelligence requirements. Once the raw data has been collected it can be processed / evaluated including assessing it against a criterion of threat, risk, harm and priorities to become information. The Home Office defines intelligence as 'assessed information', so analysis will then be performed on the processed information. This requires research and intelligence development, which results in intelligence assessments at both strategic and tactical levels, such as the SIA. This will then be disseminated to the correct recipients.

Integration then allows the NHSCFA and its stakeholders to determine how we are going to respond to fraudsters and disrupt criminal activity across the sector based on the intelligence provided within the assessments, whilst also feeding back into decision making on future priorities. As a result, the SIA has a designated place within an intelligence led organisation and can be used both internally and externally to drive overt activity to combat described threats and minimise the highlighted intelligence gaps. This ensures an intelligence[i] led response to fraud in the NHS to drive forward counter fraud activity and protect money for patient care.

Over the past year we have continued to expand and improve our working relationships within the counter- fraud community, collaborating with stakeholders internally and externally to further combat fraud against the NHS, including Project Athena data scientists and our newly embedded Fraud Risk team.

[i] This assessment is based on intelligence, data and information from various sources, therefore the hypothesis and inferences drawn are from the most appropriate and accessible / available information at the time of writing.

We have also worked with multiple external stakeholders, including NHSE, to improve our knowledge around data manipulation and pharmaceutical contractor fraud, whilst maintaining relations with policy holders, including the Department of Health and Social Care (DHSC) regarding reciprocal healthcare fraud and fraudulent access to NHS care from overseas visitors. We continue to bring more accurate and informed intelligence to the health sector. Both newly established and continuous stakeholder relations have not only increased confidence in our analysis but maintained the reliability and accuracy.

How do we calculate fraud vulnerability?

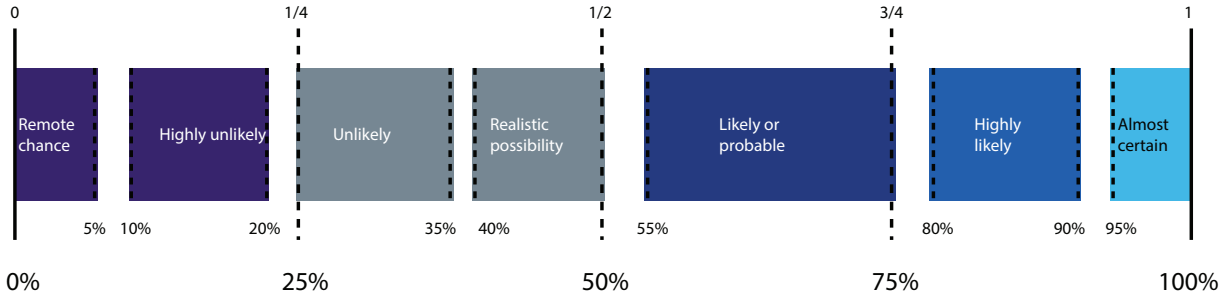
The Fraud Act of 2006 states a person is in breach if they intend 'to cause loss to another or to expose another to a risk of loss ', therefore there does not have to be a financial loss for fraud to have taken place, exposing the NHS to the risk of loss is still considered to be fraud. We need to examine direct losses, as well as where the NHS may be at risk of loss. By capturing the estimated financial vulnerabilities in thematic areas, the NHSCFA and stakeholders can develop robust prevention strategies to prevent actual financial losses from fraud.

Various methods are used to calculate how financially vulnerable each thematic area is to fraud, bribery, and corruption and in some instances, methods are combined. The loss method applied to a thematic area is dependent on stakeholder engagement, available data, landscape, process, and policy. Methods include:

- **Loss measurement exercises -** These take the form of an in-depth analysis and measurement of a particular area to provide a statistically robust percentage of how much funding/reimbursement is vulnerable to fraud. This method provides the NHSCFA with the highest confidence.
- **Comparative loss assessments -** Where the NHSCFA has not directly measured the financial vulnerability, we are reliant on vulnerability percentages derived from partners or stakeholders. These would not be 100% comparable, however they are the most relevant without a loss measurement exercise available.
- **Collaboration with policy holders -** Where a percentage of fraudulent activity is established through the study of recent data, legislation, and changes to landscape.
- **Baseline financial vulnerability rate -** A legacy percentage of fraudulent activity which is applied due to no availability of a recent loss assessment, comparative loss assessment or guidance from policy holders. Improvements could be made through stakeholder collaboration.

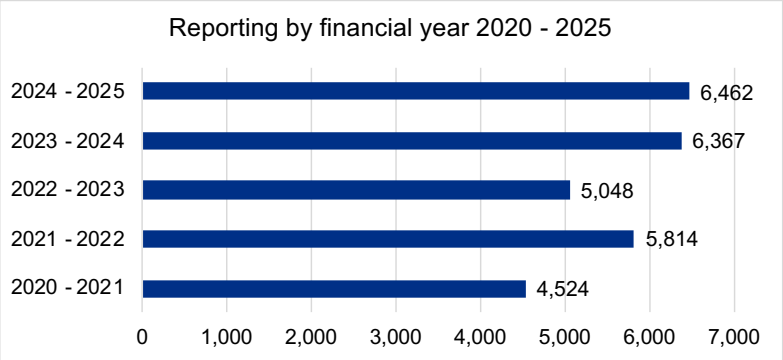
The probability yardstick

To ensure a consistent approach to assessing the probability and/or uncertainty of reports and intelligence detailed within the SIA, the NHSCFA uses the 'probability yardstick'. When using the measure of probability, the NHSCFA has considered the source, age and frequency of reporting around a common theme / MO.



Reporting trends

Between 2024 – 2025, the NHSCFA received a total of 6,462 reports alleging fraud, bribery, and corruption against the NHS in England. This is a slight increase when compared with the 6,367 reports received between 2023 - 2024.



There was an increase of 95 reports compared with 2023 - 2024. It is possible that with 59% of people in 2024 reporting they are dissatisfied with the NHS, individuals may look for ways to improve the situation, including through reporting fraudulent activity. Furthermore, the cost-of-living crisis and global landscape could influence reporting patterns.

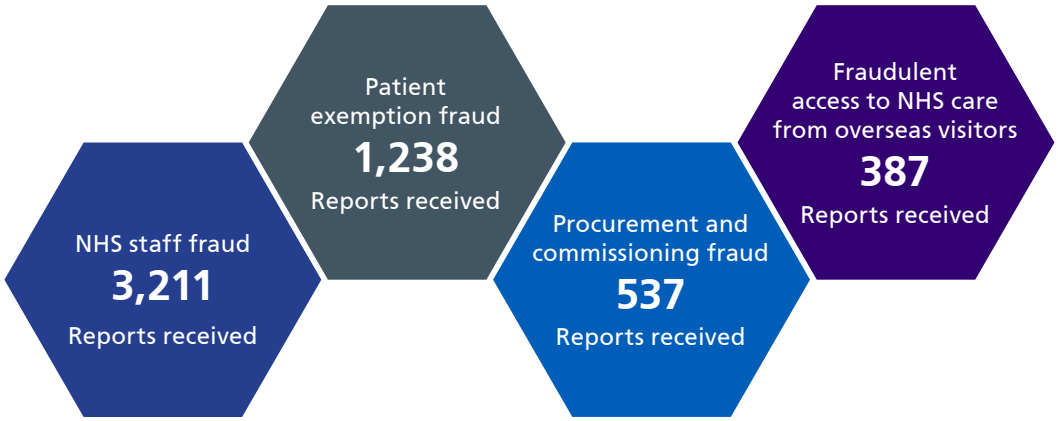
Thematic area	2020-2021	2021-2022	2022-2023	2023-2024	2024-2025
Data manipulation	14	16	13	8	25
Dental contractor	91	85	74	63	74
Fraudulent access	290	310	297	405	387
GP contractor	149	160	173	183	233
NHS Bursary	26	19	57	54	23
NHS Pensions	16	12	25	28	31
NHS staff	1,828	2,375	2,537	2,963	3,211
Optical contractor	11	24	22	28	41
Patient exemption	912	1,056	871	1,404	1,238
Pharmaceutical contractor	107	157	99	201	238
Procurement and commissioning	528	1,210	645	723	537
Reciprocal healthcare	21	11	4	7	6

blue = top four highest reporting levels

grey = an increase in reporting compared to the previous year

Top four reported areas

The NHSCFA received 6,462 reports in 2024 – 2025, of which approximately 83.2% related to the top four thematic areas of NHS staff fraud, patient exemption fraud, procurement and commissioning fraud, and fraudulent access to NHS care from overseas visitors.



Reporting has increased by around 1.5% when compared with 2023 - 2024, an increase in all but five thematic areas: patient exemption fraud, procurement and commissioning fraud, fraudulent access to NHS care from overseas visitors, NHS bursary fraud, and reciprocal healthcare fraud. Although, as mentioned above three of these areas remain in the top highest reported areas for 2024 - 2025.

NHS staff fraud continues to be the area with the highest reporting figure of 3,211, showing an increase of 8.4% when compared to the previous year 2023 – 2024 receiving 2,963 reports. Reporting equates to almost 50% of all the reports received by the NHSCFA between 2024 – 2025 and could be a direct result of oversight from colleagues and the public/patients. Of the 3,211 reports, false income and hours accounted for 62.6%, suspicious insider activity accounted for 16.2%, and declaration accounted for 9.7%. The highest reported MO within staff fraud were staff:

- working whilst on sick leave
- inflating income by falsely claiming for hours and services not worked
- working elsewhere during NHS contracted hours
- presenting false references, qualifications, and medical certificates during the recruitment process

The second highest level of reports received was within patient exemption fraud with 1,238, a decrease of 11.8% compared to the 2023 - 2024. However, in 2023 – 2024 reporting had increased which was likely due to patient registration anomalies and suspected identity fraud reports being received because of vaccination letters mistakenly being sent to incorrect addresses.

The onward trade of prescription medication for personal gain was one of the most prevalent MOs, with 27.8% of reports relating to patients legitimately obtaining prescriptions for controlled drugs and intentionally selling unwanted or unused medication, or exchanging them for more commonly misused recreational drugs, with use of another person's identity also highly reported this annum. Another trend occurring was charge evasion, whereby patients intentionally evade charges for paid NHS services like Prescriptions, Dental treatment and Optical costs, with 91.5% of these reports relating exclusively to Prescription charge evasion.

Reporting for procurement and commissioning of services fraud has decreased from 723 reports to 537, this may be due to an increased awareness through NHSCFA interventions, such as fraud reference guides. Priority projects could have impacted on reporting through more effective oversight and deterrence. This decrease can be seen within post contract reports, with the largest changes in false invoices and false validation. There has been a decrease in unsolicited requests which incorporates allegations of false invoices, phishing emails, telephone calls and office supply scams. These fraud types have been previously signposted by the NHSCFA as potential areas of vulnerability. Similarly, mandate fraud reporting has decreased. Conversely, allegations around telephone scams, fraudulent text messages and misuse of the NHS logo, have increased to the highest levels in the past five years. Pre-tender fraud areas, such as staff and contractor collusion have consistent reporting numbers over the previous five years.

Fraudulent access to NHS care from overseas visitors has experienced a decrease when compared to the previous annum of 405 reports. Individuals returning to/ entering the UK with the specific intent of accessing secondary care without charge was the most reported MO in this thematic area, making up around half of the total number of reports. Individuals falsely representing themselves to gain access to NHS care without charge whilst in the UK was the next highest reported MO. Receiving primary care, including prescriptions, whilst residing abroad was reported to be occurring.

Cyber-facilitated fraud

The government defines cyber-facilitated fraud as a 'deception to make a gain, or cause a loss, in relation to money, services, property or goods, which uses data or access obtained through cyber breaches or attacks'. The most common enabler is reported to be phishing, but others include ransomware, spyware, malware, hacking including online takeovers, and denial of service attacks.

In 2017 the NHS was one of the largest victims of the WannaCry ransomware attack which impacted not only desktops, but also medical equipment. Ransomware is malicious software which can block access to a computer system until a ransom is paid or the system otherwise restored. It has the potential to impact on patient care with appointments being delayed or cancelled and, in some cases, affect patient safety as mortality rates can increase. The Cyber Security and infrastructure Security Agency (CISA) have published warnings of credible threats of cybercrime towards US hospitals and healthcare providers with TrickBot and BazarLoader malware disseminated via phishing campaigns, which have the potential to lead to ransomware attacks and service disruption, as well as data theft.

Health data is perceived to be some of the most sensitive data and now has the potential to be more valuable than banking data on the dark web. In the last few years data thieves have been attracted by the prospect of exploiting medical data due to its value, with medical records reportedly sold on the dark web for up to $1,000. In comparison, details of a credit or debit card can be sold for between $5-110, with the difference potentially due to the ability to change banking data when it has been compromised, whereas an individual's health history cannot be altered.

This means the NHS and other healthcare agencies are potentially valuable and profitable targets for cyber criminals with medical data stolen for extortion or for impersonation and identity theft. Therefore, not only does the NHS have to be conscious of cyber enabled attacks, including attempts to steal medical data, but also of the potential for stolen data to be used to commit fraud against it. This can take the form of a phishing scam or a patient impersonating another in an attempt to gain access to NHS care, including illegally obtaining prescription medication. This could directly impact genuine patients as their medical records may come to contain information relevant to another individuals, potentially causing harm or delaying care. Furthermore, a patient who may have been chargeable but who used the identity of an individual entitled to care without charge will be leaving the NHS with a financial deficit.

The NHSE Cyber Security Operations Centre (CSOC) is responsible for protecting healthcare systems from cyber-attacks 365 days a year. They provide an early warning system for potential threats to the NHS and health sector organisations in the form of cyber alerts. A wide range of threat intelligence feeds are monitored, intelligence is collated, and alerts are triaged, with dedicated resources on the team who go hunting for threats.

The NHSCFA actively monitors and gathers threat intelligence from multiple sources relating to cyber threats, from within the NHS as well as public and commercial threat intelligence feeds to protect the organisation. We also have an ongoing programme for all our employees to raise security awareness and improve resilience and resistance to cyber threats and attacks.

Procurement and commissioning of services fraud

Procurement and commissioning of services fraud is a term used to describe pre-tender activity, the commissioning process, post-tender activity and mandate fraud.

The increase in the amount financially vulnerable to fraud compared to last year is explained by an increase in procurement spending. This is due to increases in clinical expenditure driven by inflation and changes to drugs and devices used.

£392.5m
vulnerable from an expenditure of £35.2 billion

Strategic intelligence picture

It is almost certain that some decision-makers during the pre-tender phase may be susceptible to bribery and corruption from suppliers, utilising multiple techniques to disguise their behaviour and receive bribes; for example, private residency building work or colluding and accepting other benefits like hospitality. This may be via established methods such as single tender waivers, contract splitting; falsifying quotes and tenders; and failing to declare conflicts of interest.

It is assessed a realistic possibility that the Provider Selection Regime (PSR) may enable those in decision-making positions to avoid competitive tendering by arguing that a change of current supplier is not required, or a supplier for a new contract has already been identified. As such, procurers and suppliers may become more susceptible and/or tempted to bribery and collusion by hiding behind the auspices of PSR.

As a result of the Health and Care Act 2022, the transferring of responsibilities from Clinical Commissioning Groups to Integrated Care Boards (ICBs) may now mean that unscrupulous behaviour by those in decision-making positions and/or suppliers will likely impact larger populations than before.

It is highly likely that bribery of some NHS staff may occur at both the procurement and monitoring phases of the commissioning cycle as those staff members may be tempted to accept a bribe or initiate the idea with the supplier that they can be bribed. This means the supplier could initiate the bribe to secure the contract or for the contract to continue despite performance issues.

Pre-tender fraud can also exist by contractors colluding and manipulating the bidding process through a variety of practices, such as bid rotation, bid suppression[j]

[j] Bid rotation and bid suppression are forms of bid rigging within the procurement process

and kickbacks[k]. As this occurs outside of the NHS arena it could likely result in the NHS paying more than necessary or receiving lower quality products and services. Similarly, change has occurred with the Procurement Act 2023 which now allows all suppliers, irrespective of size and how established they are, to compete for public contracts through a centralised application and tender process. These rule changes significantly increase transparency of NHS trusts as there appears to be increased emphasis on the final stage of the commissioning cycle, which could lead to negating some of the threat of post-tender fraud. However, there is a remote chance that opening the process to all suppliers could increase the potential for fraudulent practice.

It is likely for pre-tender fraud to occur if frameworks and thresholds are circumnavigated. However, a lack of oversight and contract management can enable spend to exceed thresholds. Vulnerabilities to fraud and error will likely be exacerbated as procurement thresholds have increased.

It is almost certain that the threat of payment diversion fraud, or mandate fraud, remains with instances of cyber enabled fraud by criminals to divert genuine payments or falsify payments. This will include phishing email communications purporting to be from suppliers and NHS staff, such as CEOs, to change bank account details.

Post-tender fraud extends to unsolicited requests where criminals use office supply scam invoicing to contact NHS organisations. This may be for items not received by the organisation; or indeed wanted; or the organisation has been sent inferior products but charged an inflated fee.

It is assessed as highly likely there will be continued reliance on external agencies to provide healthcare provisions. The threat of commissioning of services fraud is especially prevalent for NHS organisations when providing sufficient staffing levels through the procurement of agency staff.

However, flexibility for trusts to take the 'break glass' option and procure off-framework continues as the NHS will prioritise patient care and safety over cost, which could be manipulated for financial gain. As such, there may be ongoing collusion between employment agencies and non-framework agencies to fill vacant shifts and charge a significantly inflated rate.

Fraud may extend to agencies sending staff into the NHS who

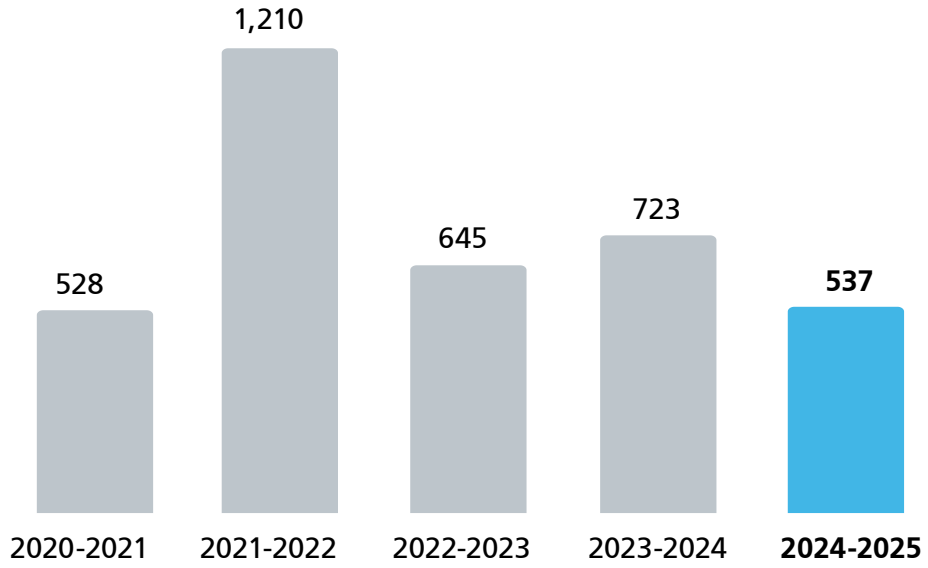
- are inadequately trained
- are under qualified
- lack specialist knowledge for the role
- carry fake documents
- are working beyond the hours their status allows

[k] Kickbacks are a form of bribery

Information reports received for procurement and commissioning of services fraud

The change in the number of fraud reports received in relation to procurement and commissioning fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

It has been announced that over the next two years NHS England will be merged with the DHSC , however this may impact how some commissioning is conducted in the future, possibly causing delays to reforms and projects. Also, as ICBs are required to reduce running costs by 50% during 2025 – 2026, it is yet unclear how this would impact procurement and commissioning processes and freedoms they have held since the reforms of the Health and Social Care Act 2012. However, the government's review of the New Hospital Programme (NHP) will see an increase in funding up to £15 billion over each consecutive five-year period from 2030. Additionally, the seven RAAC hospitals will continue to be prioritised.

The government and NHSE have proposed to reduce agency staff expenditure and reliance against the backdrop of an agency staff spending cap. They have also proposed that organisations such as the NHS take overt steps to prevent modern slavery in their operations and supply chains. This will require the NHS to liaise with suppliers to review that supply chain risk to modern slavery is mitigated and practices are improved.

The 10 Year Health Plan published in July 2025 sets out the intention to deliver a shift towards a more digital, community-based and preventative NHS by 2035, including to centralise decision-making and purchasing of technology.

Patient exemption fraud

Patient exemption fraud covers a range of abuses within NHS services that require payment upfront in return for access, including within prescriptions, dentistry and ophthalmology. It also encompasses the onward sale or supply of prescribed medication.

£230.2m
vulnerable from an expenditure of £11.8 billion

The financial vulnerability has decreased compared to the previous year. However, this is not indicative of a decrease in threat and is because of a change of data parameters used last year. Therefore, due to differences within the previous data set the figure is not comparable.

Strategic intelligence picture

The onward trade of prescription medication for personal gain remains highly likely in this area. This can involve selling unwanted or unused medications as well as intentionally obtaining controlled medications via deception e.g. by feigning illness or injury to specifically obtain and sell prescribed items for profit, particularly in lucrative markets abroad. An emerging trend identified was the onward trade of prescriptions relating to weight-loss.

Theft of identity to register for NHS services or medication is highly likely in this thematic area. This MO is most commonly linked to individuals who have entered the UK unlawfully using false identities, stolen identities or identities of their friends or family who have legal status in order to avoid detection. This is enabled by the misconception that they are not entitled to any NHS treatment without charge, or concerns that the NHS may pass their details to Immigration Enforcement. There have been several noted links in using repeated false identities or addresses to claim for state benefits, like Universal Credit, and claiming or registering for NHS services.

Patient charge evasion remains highly likely in this area. This involves patients deliberately and intentionally avoiding charges for services which require payment in the NHS, like prescriptions, dentistry and optical costs. The NHS offers a Low Income Scheme (LIS) as a means tested assessment for patients to demonstrate low income and gain an exemption for NHS charges. However, it is a realistic possibility that some patients withhold some information to qualify for the scheme.

Real-Time Exemption Checking (RTEC)[I] continues to have a positive effect on charge evasion. However, there were unsuccessful matches at the point of dispensing resulting in challenging the patient or a Penalty Charge Notice (PCN) being issued

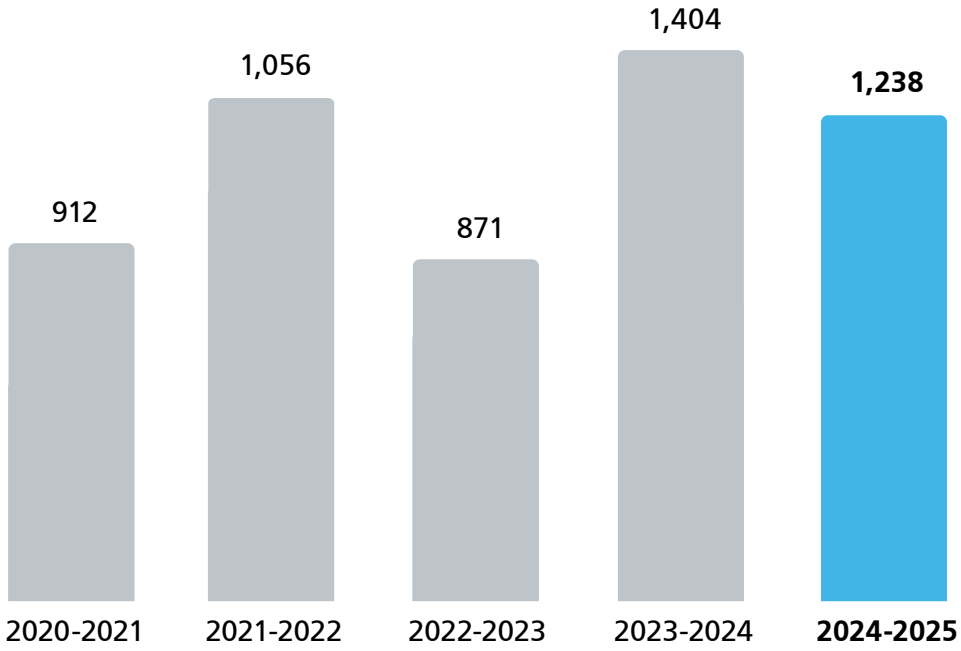
[I] RTEC enables pharmacies to determine whether an individual is exempt or chargeable for a prescription.

by the NHS Business Services Authority (NHSBSA) to recover the loss. There is the possibility that unsuccessful validations may go unchecked 'real-time' by pharmacists in order to avoid potential conflict with the patient or speed up dispensing. There could also be some confusion amongst patients receiving Universal Credit, who may not be aware that receiving Universal Credit alone does not necessarily equate to free prescriptions, dental treatment and optical costs.

Information reports received for patient exemption fraud

The change in the number of fraud reports received in relation to patient exemption fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

Under plans introduced in February 2024 to recover NHS dentistry, dentists will be offered incentives to take on new NHS appointments, with the aim to create an additional 2.5 million NHS dentistry appointments or 1.5 million NHS dentistry treatments. Under the plan the minimum Units of Dental Activity (UDA) rate will be raised, with the aim of making NHS work more attractive and sustainable. This could in-turn lead to an increase in those having NHS dental appointments, which could impact on reporting of charge evasion.

Data manipulation fraud

Data manipulation includes falsifying data to meet targets, increase revenue or hiding undesirable outcomes, including within A&E. It encompasses the '2023 - 2025 NHS Payment Scheme' (NHSPS) and the four different payment mechanisms it governs within secondary care.

£189.1m
vulnerable from an expenditure of £63 billion

The financial vulnerability estimate has increased because of the increase in the funding allocated to ICB core services and elective recovery care funding compared to the previous year.

Strategic intelligence picture

There is the potential to manipulate performance data and accounts within an NHS Trust to meet cost improvement targets. Potentially enabled if senior management request staff submit false accounting figures, request suppliers issue invoices before a cut off, cancel invoices with credit notes, create false provisions to meet targets, and increase purchase orders with the intent of reducing them in the future.

It is a realistic possibility for performance data to be falsified with the intention of meeting targets in advance of multiple tendering processes. Staff could be instructed to input the date of when an appointment was booked into a system instead of when the appointment was due. Thus, allowing the appointments to appear compliant when targets were not actually being met.

There is the potential to falsify statistics to ensure monthly targets are met for patients being discharged. Management could instruct clinicians to delay discharging specific patients during certain months which could impact on targets.

It is probable that some medical staff could claim to provide programmed activities at an NHS trust and receive payment, yet not perform these services. This is potentially enabled through the conduct of these individuals being omitted by senior management. Furthermore, there is the potential to submit false information around a compliance inspection without accessing the relevant location.

A Trust has the ability to manipulate data to appear as if there is high utilisation of hospital facilities. By closing lists which are not filled and then excluding them from reporting, the metrics can be manipulated to appear as if there is high utilisation of certain facilities.

It is likely that trusts are manipulating performance data to appear as if they are delivering higher levels of performance or improvement. These manipulations can

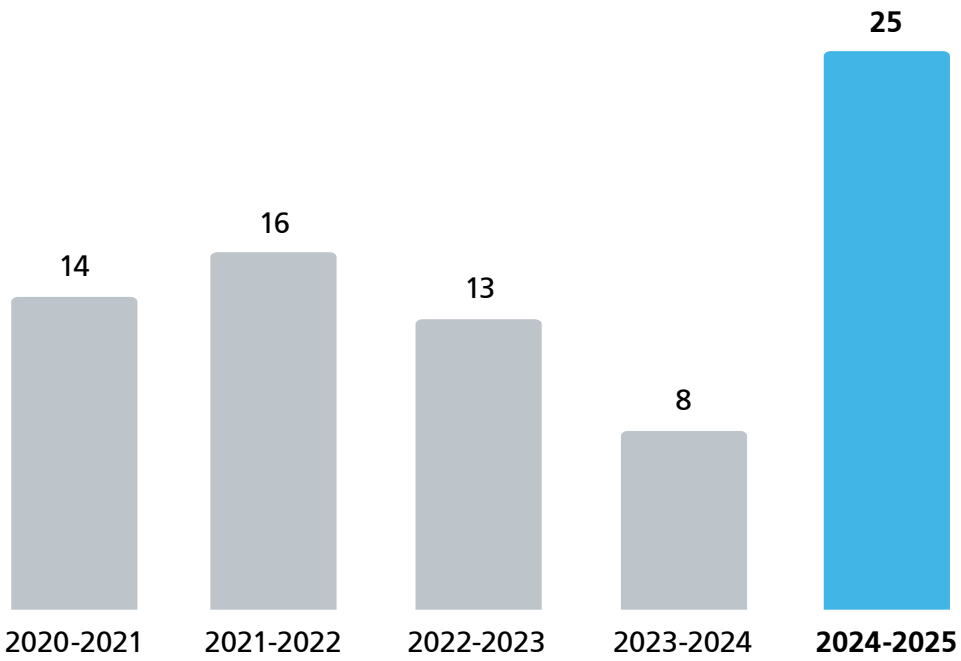
result in a financial benefit, as the acute trusts which achieved the highest-level target percentage and/or improvement for A&E 4-hour performance could receive between £1million to £4 million within the urgent and emergency care (UEC) capital incentive scheme. Managers could instruct staff in the emergency department to amend data to appear as if 4 hour waiting times have been achieved. There is also the potential to abuse the use of diagnostic holding centres or clinical decision units to avoid breaching and possibly incurring additional charges.

It is highly likely that a trust could record a patient as a day case instead of outpatient to incur additional funding. It is possible for a department in a trust to be recording appointments in a way which enables additional funding to be accrued. When patients are admitted as a day case this can attract a higher price than if they are recorded as an outpatient attendance, as a day case would be considered as an inpatient to the hospital. However, the reverse can be incentivised through setting a higher price in policy, where a day case can legitimately be recorded as outpatient.

Information reports received for data manipulation fraud

The change in the number of fraud reports received in relation to data manipulation from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

The consultation for the proposed 2025/26 NHSPS closed on the 28th of February 2025. However, the amendments which were proposed were yet to be confirmed at the time of writing this assessment, therefore the full impact was unknown. Inflation has reportedly eroded the financial allocations received by Trusts, with an inflation assumption of 2.5% in 2023 - 2024 being surpassed by a reported 6.2%.

The UK has been impacted by the baseline tariff (other than with automobiles) as part of the reciprocal tariffs introduced by the United States of America, with some other countries receiving higher tariffs. These tariffs could potentially impact on the current price caps, drug tariffs, the market forces factor (MFF) or funding allocations in the NHS.

Community pharmaceutical contractor fraud

Pharmaceutical contractor fraud involves the falsification or exaggeration of services as well as collusion.

The financial vulnerability has increased from last year and this is explained by an increase in the number of prescription items dispensed, alongside a cost per item increase[m] of 15p.

£135.2m
vulnerable from an expenditure of £13.5 billion

Strategic intelligence picture

Pharmacists are contracted to deliver essential and advanced services to the public as outlined in the Community Pharmacy Contractual Framework (CPCF). Pharmacists have a good understanding of the services they are required to carry out, as well as the reimbursement process and how to manipulate claims. Increased pressures on pharmacists to deliver more services, as well as reductions in opening hours and staffing levels, alongside a cost-of-living crisis, may impact the threat of fraud.

It is likely that some pharmacists are claiming for items which have not been dispensed or required; for example, a pharmacist claiming for these items and then placing them back onto the shelf for resale. Similarly, pharmacists may not dispense or only dispense part of a prescription and resell profitable items. This may extend to high value and sought after items such as diabetes and weight loss drugs/injections, inhalers and liquid medications.

Pharmacists may also manipulate the NHS Spine by claiming for, but not dispensing the item, resulting in the patient re-requesting the prescription from their GP. Similarly, accessing the Spine and changing the patient's nominated pharmacy without consent.

Inappropriate claiming of prescription items may extend to some pharmacists:

- dispensing incorrect strengths
- dispensing out of date medication
- swapping generic medication for branded equivalents
- claiming prescriptions for deceased patients
- charging both patients and the NHS for items when the patient is exempt and/or their normal prescription is out of stock, but an alternative is identified

[m] £8.86 increasing to £9.01

It is probable that inappropriate claiming also exists within delivery of patient services, such as New Medicine Service (NMS) and blood pressure checks, where some pharmacists may have claimed despite the patient not receiving the intervention.

There is also the realistic possibility that multiple patient services are unnecessarily claimed at the same time for the same patient. It is assessed that expansion of services such as Pharmacy First and the Hypertension Case-Finding Service, will likely present an opportunity for some to inflate activity to increase revenue.

It is assessed as likely that inappropriate claiming also exists in other funding streams such as Dispensing Appliance Contractors (DACs). Contractors can have multiple accounts with the responsibility for providing appropriate and sufficient appliances, as well as a remit of providing services in emergency situations. As such, they may manipulate claims to shift prescriptions between accounts and maximise infrastructure payments.

Hitting monetary incentivised targets makes services potentially vulnerable to manipulation. As such, contractors may falsify claims to achieve an activity threshold to receive a payment. Similarly, the introduction of quarterly caps based on service delivery from an earlier period may have increased the threat of claiming manipulations. This may also include falsifying patient details including inventing "ghost patients"; or misrepresenting a brief conversation with a patient as a private consultation in a secure room. In the case of Pharmacy First, manipulations could extend to pharmacists prescribing for different conditions to those approved under the scheme.

It is a realistic possibility that adopting a target-driven approach to generate profit and hit monetary incentives could also result in staff being coerced. Applying coercion on staff may extend to claiming but not dispensing items to patients and staff inflating activity by carrying out patient services on associates and other staff members. Applying such tactics may be more prevalent within commercial chains and may lead to greater vulnerability as they are likely to be used by more patients.

Public awareness of the specific requirements for some services offered to them may also enable manipulation of claiming behaviour. As such, the patient may be unaware as to whether they have received the service fully, partially or at all. The patient may also not know if the service was necessary, and they may not have consented if they were aware of the fee paid to the pharmacy directly from the NHS for its administration.

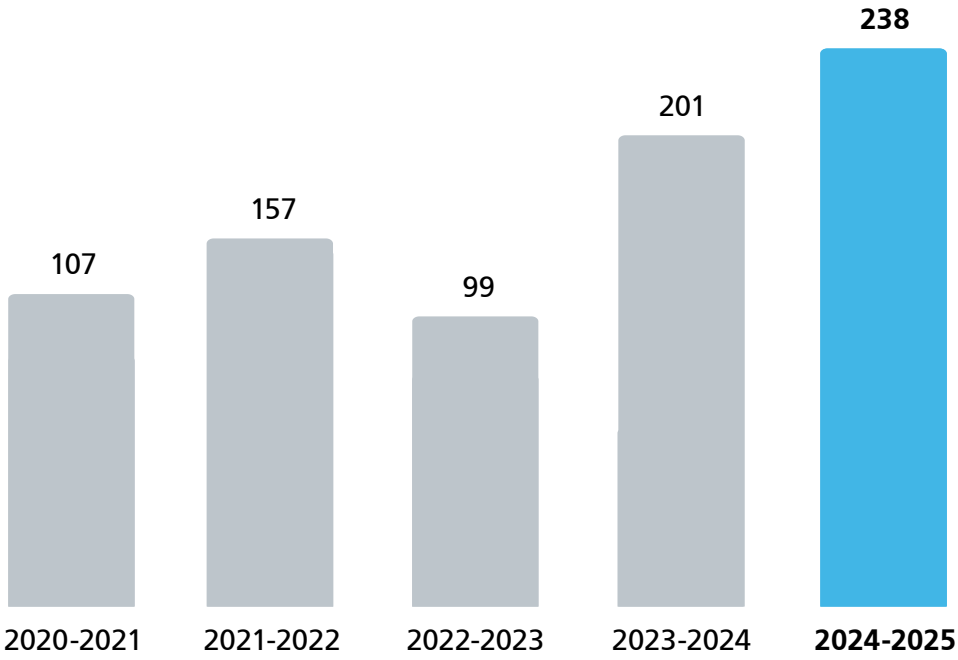
Manipulation of fee payable services and items extend to specific medicines, such as 'Specials', and patient service areas such as out of pocket expenses (OOPE) where it is a realistic possibility that pharmacists and manufacturers may collude and split profit through.

Capacity issues within community pharmacies may also be an emerging vulnerability that leads to manipulation of claiming behaviour of both prescription items and patient services. Some contractors may feel added temptation to remain viable business models.

Information reports received for pharmaceutical contractor fraud

The change in the number of fraud reports received in relation to pharmaceutical contractor fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

The CPCF five-year framework concluded at the end of the 2023 – 2024 financial year, therefore, the Department of Health and Social Care, NHS England (NHSE) and Community Pharmacy England have been negotiating new funding streams throughout 2024 – 2025 and the following year's contractual framework.

Separate to the CPCF framework, this reporting period contains the second year of a £645 million investment for a major expansion in primary care access in community pharmacy. This has included the Pharmacy First initiative, an expansion of the pharmaceutical remit so patients can obtain prescription medication for common conditions, such as urinary tract infections.

Contractors must also provide Contraception and Hypertension Case-Finding services to qualify for £1,000 monthly payments. This is against the backdrop of future aspiration within Pharmacy First where an expansion of the service has been touted and estimated to free up GP appointments.

The second half of the 2024 – 2025 financial year has also seen the introduction of quarterly Pharmacy First caps, based on service delivery from a previous three-month period in the year.

General Practice (GP) contractor fraud

Fraud relating to the manipulation of income streams or activities that violate contractual terms perpetrated by either GPs or practice staff.

£116.7m
vulnerable from an expenditure of £11.6 billion

Financial vulnerability in this area has increased compared to the previous financial year. However, it is assessed that this increase is not necessarily indicative of an increase in fraud and is more in-line with the increase in expenditure paid by the NHS to general practitioners this financial year. Due to data anomalies, a different methodology was used to calculate financial vulnerability compared to previous assessments.

Strategic intelligence picture

Claiming and receiving funding for services not provided is likely in this area. This is where GPs or Primary Care Networks (PCNs) intentionally claim for funding to provide additional services, which are then not provided to the public as agreed contractually. Funding is provided by Integrated Care Boards (ICBs) from the NHS, direct to PCNs based on weighted population, where it can be used to reimburse the cost of hiring some additional roles to support the day-to-day workload of GPs, such as paramedics covering GP appointments. In some instances, this funding was diverted elsewhere to fund other ineligible services, top up core-staff wages, or siphoned for personal profit by senior partners in GP practices.

Diversion of practice funds, involving the manipulation of salaries and payroll is also prevalent in this area. This can involve the incorrect allocation of core 'Global Sum' funding provided by the NHS as well as senior members of staff at practices diverting or siphoning funding allocated for salaries, staff pensions and other payroll requirements for personal gain. The overall seniority and authority these GPs, partners or staff members, have in the General Practice model creates vulnerability as this enables them to move these funds away from the practice with little scrutiny or challenge, preventing whistle blowing and encouraging collusion through complicity to remain in employment.

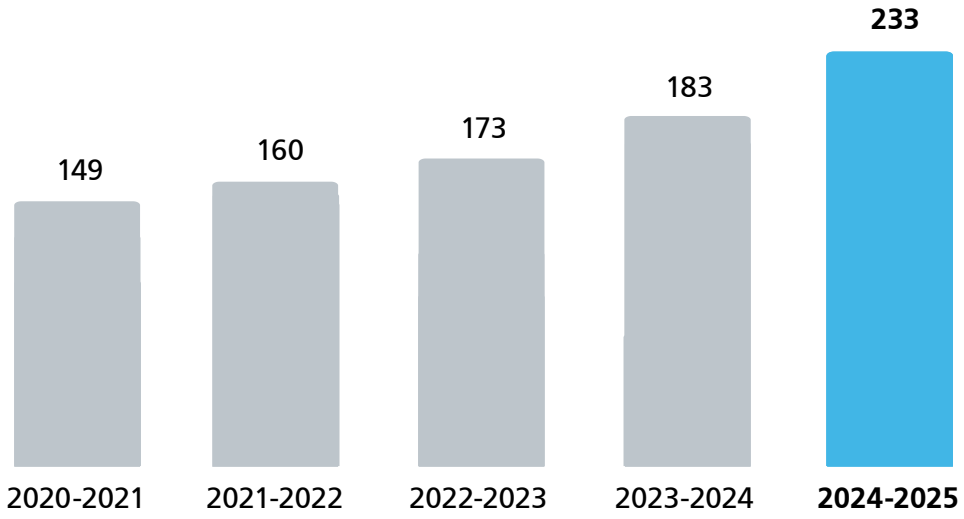
Another prevalent MO identified in this thematic area is the abuse of position by GPs and other senior practice staff to enable their own personal or professional gain at the expense of the NHS. This includes abusing access to controlled medications in order to self-prescribe for personal misuse, or onward trade for personal gain. This can include the use of the information of deceased or ex-patients who have moved area. Again, this activity is vulnerable due to the seniority and authority held by GPs and high-ranking staff members within the GP model.

Further to this, an emerging MO identified as part of this category is the redirection of patients to pharmacies in which they have an undeclared business interest, to increase activity and claim the maximum amount possible from the NHS. This professional gain for the pharmacy in-turn allows for personal gain through increased turnover which may constitute a conflict of interest.

Information reports received for General Practice contractor fraud

The change in the number of fraud reports received in relation to GP practice fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

The British Medical Association (BMA) has backed a UK-wide extension of salaried GP maternity leave benefits, whereby funding would be made available for all GP surgeries based on their patient size list for these salaries to be drawn out of. There is potential for fraud if outgoings on salaries were to increase.

A new NHS neighbourhood model could drive an overhaul of GP contract funding, which could create emerging threats and enablers of GP fraud for the NHS.

Optical contractor fraud

Optical contractor fraud involves submitting claims to the NHS for optical treatments, services, or enhancements not delivered or clinically required.

The decrease in the amount financially vulnerable to fraud bribery and corruption can be attributed to a decrease in expenditure.

£90.7m
vulnerable from an expenditure of £564.5 billion

Strategic intelligence picture

There is the possibility that contractors are prescribing spectacles to vulnerable care home residents and children without consulting their next of kin. Including not performing a genuine eye test on care home residents and claiming for two pairs of spectacles. Potentially occurring when there is reduced oversight.

Submission of fraudulent General Ophthalmic Services (GOS) 1, 2 and 3[n] claims for ghost patients, or patients who did not require NHS services or treatment, or never attended for eye tests or spectacles is likely. False GOS claims for patient services which were not provided or clinically required was also identified, in addition, manipulation of prescriptions to claim for higher value GOS payments, double claiming for appointments by splitting treatments or submitting multiple claims for the same voucher was also noted.

There is the potential for ophthalmologists to charge eligible patients and simultaneously submit a GOS claim for the same service, or charge extra on top of the GOS vouchers for financial gain. Additionally, there is the potential for ophthalmologists to be claiming reimbursements from the NHS for private patients, or those who are ineligible for free NHS eye tests or vouchers.

Use of false or fraudulent signatures to submit GOS claims is a realistic possibility. There is the potential for an optical branch to use the signatures of practitioners who are no longer employed by the practice for GOS forms or to submit false claims for those exempt from charge with fraudulent signatures.

An emerging threat included Optical practices which did not hold an NHS contract submitting their claims through a practice in another area which does hold an NHS contract. Potentially enabled through staff at the practice altering the claims or collusion.

The International Council of Ophthalmology (ICO) certificate is given to successful candidates who pass the ICO Advanced Examination. However, there is a realistic

[n] NHS optical vouchers help eligible patients cover the cost of spectacles or contact lenses.

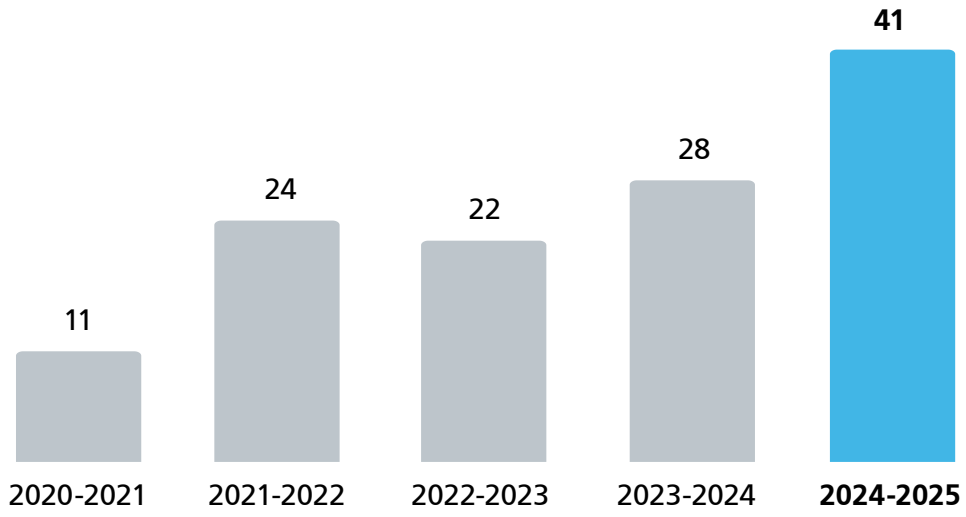
possibility that an applicant could submit false documentation to an ICB when applying for a contract to provide GOS.

An ophthalmology consultant could perform private work in a private hospital yet issue FP10[o] prescriptions to private patients. Also in secondary care, there is a remote chance that a patient could pay for an item which was not provided, with no payment record appearing on the hospitals financial system.

Information reports received for optical contractor fraud

The change in the number of fraud reports received in relation to optical contractor fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

The media has reported on the introduction of 10% tariffs on UK imports to the USA, this could indirectly affect NHS optical services. While medicines are currently exempt from tax at the time of writing this assessment, some medical equipment and supplies used in NHS optical services may become more expensive. Future costs of treatment may also increase due to increased cost in the supply chain. This could potentially lead to higher prices for optical equipment and delays in services.

[o] An FP10 is a prescription form

Dental contractor fraud

NHS dental services in England are provided by dental practitioners under contract to deliver general care and treatment. Dental contractor fraud concerns the fraudulent claims submitted to the NHS by dentists and their staff members for a range of NHS services provided to patients.

£57.6m
vulnerable from an expenditure of £3.06 billion

The amount financially vulnerable to fraud bribery and corruption in this thematic area has seen a decrease, which can be attributed to a reduction in contracted Units of Dental Activity (UDAs), expenditure for General Dental Services (GDS) and contract providers.

Strategic intelligence picture

Dental practices submitting false claims for exempt patients remains a probable threat in this thematic area. Potentially enabled by staff accessing patient records on the practice specific system, submitting false claims and falsifying exemption forms.

The manipulation of activity data through altering Units of Dental Activity (UDAs) and patient data to secure additional funding is likely. For example, overcharging NHS patients or splitting courses of treatment to submit multiple claims to the NHS.

In order to boost revenue, it is possible for a contractor at a dental practice to falsely claim for mouthguards that are not necessary and were never fitted to patients. Additionally, a dentist could potentially claim for dental procedures which were not undertaken to claim the maximum of 5 units of dental activity. Dental contractors may also generate false claims to the NHS, where the patient has paid privately, to claim a double income.

It is a realistic possibility that dental practices may onboard NHS patients with the intent of receiving payment but not offering appointments. From March 2024, the government introduced the 'new patient premium' to deliver additional dental appointments, where extra payments are made for seeing new NHS patients. Therefore, a dental practice could recruit NHS patients, offer NHS appointments and then cancel them last minute, but continue to take on private work.

At present, overseas dentists are required to pass an exam before they can start work in the UK. However, currently there is the potential for contractors to employ overseas dentists and allow them to treat patients without the relevant training or qualifications.

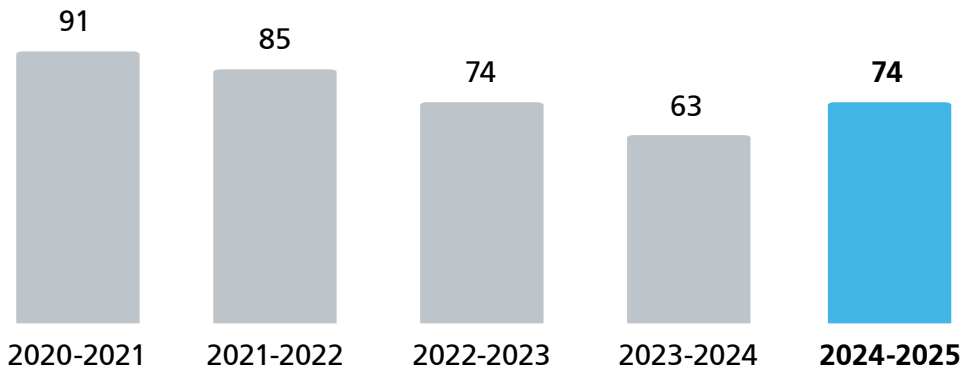
Dentists within a hospital may be able to manipulate data to claim extra payments. Trusts may also restrict the flow of patients through the service by insisting every patient is seen by a consultant at each stage. Resulting in overtime payments and waiting list initiative payments for reducing the backlog created.

Dental contractors carrying out unnecessary treatments also remain likely in this area. Dental contractors could perform unnecessary dental work to claim for treatments in a higher banding. This could be enabled by contractors having the authority over what treatment a patient needs, enabling them to undertake false treatments and manipulating the patients' record on the system.

Information reports received for dental contractor fraud

The change in the number of fraud reports received in relation to Dental contractor fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

Under the dental recovery plan dentists will be offered a 'new patient' payment with the aim of creating more than 2.5 million NHS appointments. Under the plan the minimum Units of Dental Activity (UDA) rate will be implemented, with the ambition of making NHS work more attractive and sustainable.

With the limited access to NHS dentistry, mobile dentistry vans were introduced to visit rural and coastal communities known as "dental deserts", areas where patients struggle to access NHS dentists. It is possible that as mobile dentistry is rolled out more, it could attract fraudulent activity by the contractors, using the popularity, numbers and limited supervision to create false claims.

NHS staff fraud

NHS staff fraud encompasses staff manipulating income and hours, insider abuses, and false representation during application processes.

The financial vulnerability has decreased due to NHS services returning to pre-COVID-19 levels. Thus, reducing the need and reliance on expensive temporary agency staff, resilience for extra pay for working in high-cost areas, working unsocial hours, and band supplements.

Strategic intelligence picture

Working elsewhere whilst on sickness leave was highly likely within NHS Staff fraud. Staff could be falsifying sickness to receive both sick pay and extended leave while fit to work, with some potentially working for other employer(s) or their own private work or business during their sickness period. Dual employment is also likely with staff working simultaneously at other NHS Trusts whilst on short / long term sickness absence, including staff working bank shifts during their contracted hours in parallel with their substantive post.

There is a remote chance that Staff on long term sickness leave could present false or manipulated Med 3 certificates or private paid certificates to justify prolonged absence and mask genuine medical need when they are genuinely well.

There is also a remote chance of clinical staff falsifying sickness to be signed off on Tier 1 ill health grounds, despite not being genuinely unwell. Tier 1 is intended for those permanently incapable of performing their clinical duties, thus highlighting some staff misusing this clearance to avoid their responsibilities while working elsewhere.

Inflation of income and hours, including claiming for hours, shifts, overtime and patient care services which were not worked was also highly likely. Some staff may be abusing their position by manipulating their timesheets and e-rostering systems to inflate their income.

Furthermore, NHS staff retrospectively booking bank shifts on the e-rostering system with the intent to fraudulently claim for payments after not having worked or having any intention to is probable. Tampering and manipulation of e-rosters is possible, including through changes to shifts and pay bands to claim higher or enhanced pay. This likely occurs with bank shifts; some in collusion or means of nepotism with senior staff knowingly signing off or allocating bank shifts on a higher pay band. Senior staff could also be granting themselves a pay band uplift for certain shifts or services.

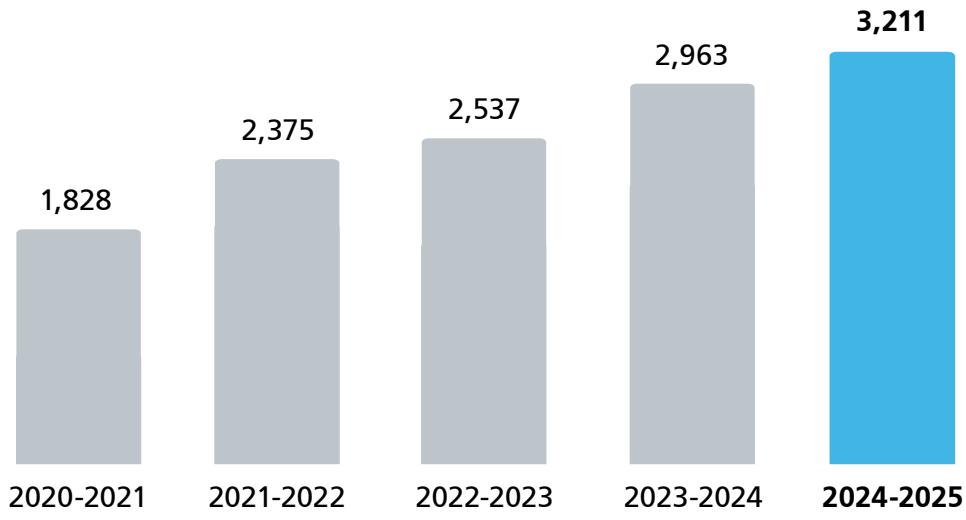
It is likely that some staff may work elsewhere during NHS contracted times, including staff working for their own private business, another NHS Trust, or an external organisation. Staff may have undeclared secondary employment including those with multiple employments, freelancing, or seeing private patients, thus leading to conflicts of interest and potential breach of contract. In addition, clinical staff could perform private paid practices / treatments, to private patients using NHS assets during their contracted times.

It is highly likely that an impersonator may use another person's ID to carry out shifts. Bank shifts could be booked in advance via e-rostering however a pre-booked shift could be carried out by another person using the staff members ID, whilst the original shift booker is completing their substantive role.

Information reports received for NHS staff fraud

The change in the number of fraud reports received in relation to NHS Staff fraud from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

The NHS in England is undergoing significant workforce reforms as part of the NHS Long Term Plan and the new NHS 10 Year Health Plan as set by the government. Including reducing reliance on agencies in the coming years by training more NHS staff domestically and retaining more existing staff. The NHS has struggled to recruit staff to meet demand and is therefore reported to have been hiring health staff from the World Health Organisation (WHO) work force support and Safeguard red list countries to meet demand. The Secretary of State for Health and Social Care is determined to reduce the NHS's reliance on recruitment from red-list countries by investing in staff through their change plan.

Reforms include NHS England merging with the DHSC and Integrated Care Boards (ICBs) being required to halve their costs. However, this will likely impact on NHS employment figures.

The Nursing and Midwifery Council (NMC) has recently highlighted a case where it is alleged that a genuine NMC registrant's identity was being used fraudulently by one or more non-registrants, for the purpose of gaining work in roles that are for registered nurses. This resulted in the NMC advising and providing guidance around the risk of identity fraud during recruitment. Similarly, Ofqual is setting out measures to strengthen steps to find, tackle and prevent qualification fraud.

Fraudulent access to NHS care from overseas visitors

The term 'fraudulent access to the NHS' refers to when a patient falsely represents themself as entitled to NHS care without charge, fails to disclose they are chargeable, or an NHS staff member who has abused their position to facilitate the fraudulent access.

£98.1m
vulnerable from an expenditure of £2 billion

The financial vulnerability estimate has continued to improve through a collaborative approach with policy holders to maintain a more accurate and up-to-date figure. The increase is reflecting a rise in general inflation and an increase in the number of visitors to the UK.

Strategic intelligence picture

Non-residents falsely representing themselves to gain access to care without charge while in the UK is ongoing and highly likely within this thematic area. There is the potential for individuals to use false documentation to prove ordinary residence in the UK. Individuals could therefore use a false identity or the identity of another individual who is entitled to care without charge to gain access to secondary care but avoid costs.

Although primary care is free to all, it is highly likely some patients will manipulate the system to receive primary care, including prescriptions, whilst residing abroad. Potentially enabled through patients failing to update their GP that they have moved abroad, use of digital prescription services and the ability to collect a prescription on behalf of another.

It is likely that individuals are returning to or entering the UK to specifically access secondary care. Potentially enabled through the use of an associate's address or a previous address to prove ordinary residence, combined with patients being registered at a GP practice, receiving an NHS number and / or use of a visitor visa.

Publicising fraudulent access to the NHS for non-ordinarily residents to access the NHS without charge is a realistic possibility. Posting a journey of accessing the NHS without charge when not entitled on a social media platform could potentially influence others who aren't eligible.

Individuals returning to or entering the UK specifically to access secondary care without charge may also be enabled through NHS staff facilitation who may unintentionally or deliberately fail to check the charge status of the patient.

NHS employees may help associates who reside abroad permanently to receive ongoing care without charge.

A&E is free to all individuals in the UK; however, any follow up treatment or specialist referrals may become chargeable. Patients can be discharged from A&E into attendance at Same Day Emergency Care (SDEC). It is possible that some individuals returning to or entering the UK specifically to access secondary care could avoid charges by accessing care via the A&E route.

There is a potential emerging issue around the misuse of visas, where individuals may gain treatment during a period and then leave the UK. If the individuals aren't detected they can continue to manipulate this system using another visa at a later date.

Misuse of visas is a realistic possibility, individuals on student or work visas could sponsor relatives with long term health conditions to come to the UK with the intent of acquiring treatment. There is also the potential for individuals to claim asylum before their visa expires to access treatment without charge available to asylum applicants.

There is an emerging issue of individuals using a private treatment medical visa to enter the UK and then later gaining NHS treatment without charge. It is possible for individuals to transfer from a private medical company to the NHS or cancel the private appointment and attend A&E instead.

It is likely that individuals will enter the UK to access maternity services in the NHS. Maternity treatment in the UK is categorised as 'urgent and necessary' meaning costs are recovered after the treatment and not before. This enables individuals to come to the UK to get treatment, then potentially leave before costs are recovered. Another vulnerability of a non-ordinarily resident giving birth in the UK (including individuals on a visa) is that the cost of a baby's care can become chargeable.

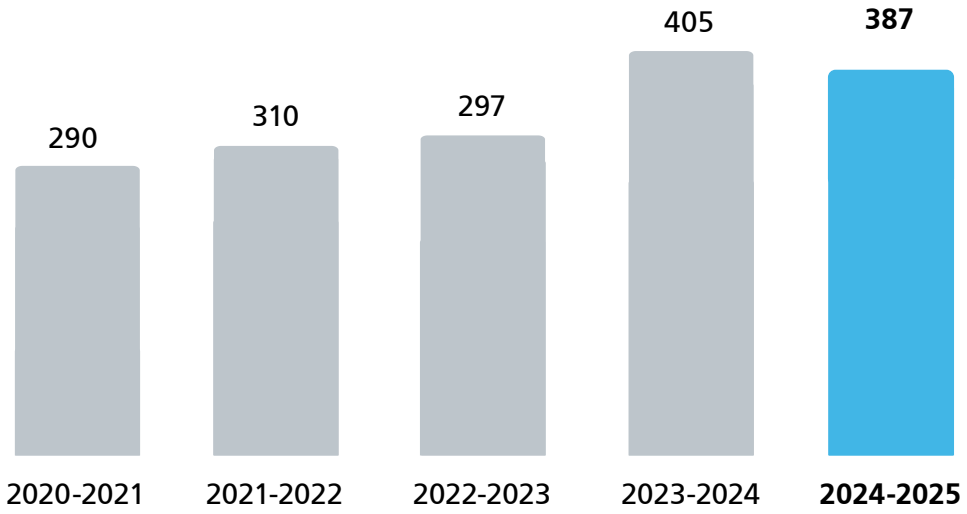
British Citizens now residing abroad who fly to the UK for treatment without an S1 or S2 demonstrates an emerging threat. Patients may keep cancelling appointments or inform staff that they have flown over for the appointment.

The National Care Records Service (NCRS) uses a traffic light score to show patients' eligibility status. If ineligible patients have the wrong code recorded, they could potentially evade charges.

Information reports received for fraudulent access to NHS care from overseas visitors

The change in the number of fraud reports received in relation to fraudulent access from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:

Reporting from 2020 - 2025



Horizon scanning

In February 2024, the Immigration Health Surcharge (IHS) fees increased by 66%, the surcharge is designed to help fund the NHS and to ensure those who come to live in the UK contribute to the cost of the healthcare services. Once the surcharge is paid, the individual will have access to most NHS services, however they may still need to pay for certain services.

In April 2025 the Electronic Travel Authorisation (ETA) was introduced in the United Kingdom, an ETA can be cancelled if an individual has outstanding charges of at least £500 owed to the NHS.

In early 2025 tariffs imposed on trading partners by the USA were announced and are likely to cause healthcare costs to increase in the USA. This could result in individuals entering the UK with the intent to fraudulently access healthcare without charge as the USA is already reported to experience one of the highest costs of healthcare in the world.

Reciprocal healthcare fraud

Reciprocal healthcare encompasses fraudulent use of European Health Insurance Card (EHIC), Global Health Insurance Cards (GHIC) Provisional Replacement Certificates (PRCs) and various other reciprocal healthcare arrangements. It also includes false representation during the application stage which can enable the card / certificate holder to benefit from a reciprocal healthcare agreement.

£824,000
vulnerable from an expenditure of £154.8 million

The financial vulnerability estimate has been improved through a continued collaborative approach with policy holders to maintain a more accurate and up-to-date figure. The estimate only encompasses EHIC, GHIC and PRC expenditure, it does not include the S1[p] scheme, the smaller S2[q] scheme or other reciprocal healthcare agreements.

The claims issued, the costs of an EHIC/GHIC application and percentage of fraud and error have increased when compared with the previous year.

Strategic intelligence picture

It is likely that some individuals, although eligible at the time of application, will fail to declare their change in circumstances when they move abroad permanently and will continue to use their UK issued EHIC/GHIC, including for planned care upon refusal of an S1 or S2.

Submitting a fraudulent application for a GHIC was also probable, with applications being made using the details of another individual.

It is likely for applications for EHIC/GHICs to come from individuals without eligibility who are permanently residing outside of the UK. This is likely enabled through use of a UK address to prove ordinary residence and a location to which the card can be dispatched, whilst an associate still residing at the address can pass on letters and parcels. As a result, the individual will be provided with UK insured healthcare for up to 5 years through an UK EHIC / GHIC whilst permanently residing abroad.

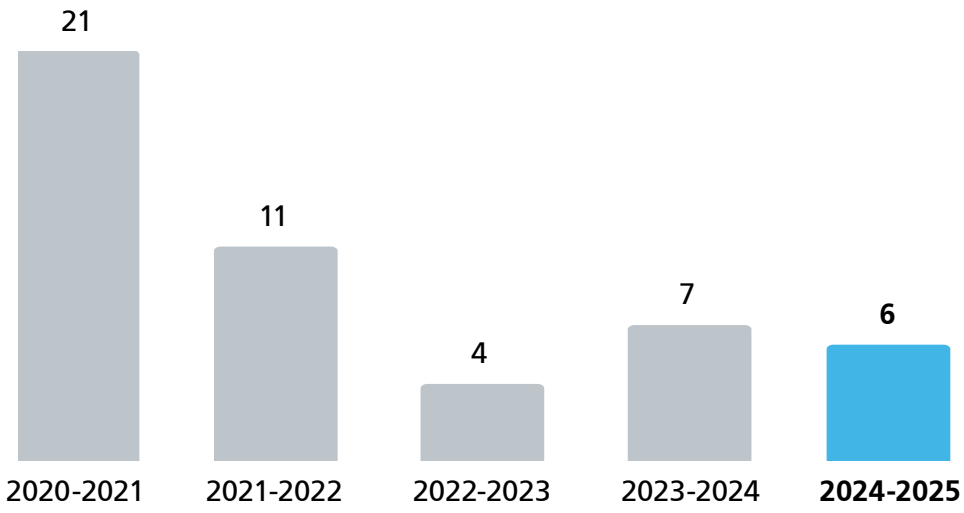
There is a realistic possibility that a trust may receive a fraudulent email impersonating an Overseas Visitor Manager (OVM). Individuals may attempt to falsely present to the trust that an OVM has confirmed the cost of care would be covered by the patients EHIC.

[p] Provides healthcare to eligible individuals living in an EU or EFTA country and constitutes the majority of reciprocal healthcare expenditure.
[q] Provides planned treatment in EU or EFTA countries for UK residents.

It is almost certain that the European Union (EU)/European Free Trade Association (EFTA) will reject some UK invoices due to fraud or error because of incorrect or missing information on the E125 form, and in some cases the individual cannot be identified. Duplications of claims or invoices are also reported to be a problem. In some cases, EHICs have expired, and individuals are not insured during all or some of the treatment period.

Information reports received for reciprocal healthcare fraud

The change in the number of fraud reports received in relation to reciprocal healthcare from 2020 - 2021 to 2024 - 2025 is illustrated in the below chart:



Horizon scanning

It is likely applications for UK EHIC/GHICs have previously been made from outside the UK even though it is a scheme based on ordinary residence unless there is an exemption. Tariffs imposed on trading partners by the United States of America could impact on healthcare costs, causing them to increase and be passed on to USA patients. Therefore, although, the threat is considered low, as cards would need to be sent to a UK address and applicants provide false evidence of UK residency, there is the potential for false GHIC/EHIC applications from those who are ordinarily resident in the USA.

Additionally, the media reports that the pharmaceutical industry is profoundly reliant on USA trade, with ingredients for life-saving medicines travelling between the USA, UK and EU. Tariffs on medical items could cause charges which are not factored into pricing caps within the NHS, potentially leaving the NHS further out of pocket when someone falsely represents themselves as entitled to care under a reciprocal healthcare agreement.

NHS
Counter Fraud Authority

10 South Colonnade
Canary Wharf
London
E14 5EA
Tel: 0207 895 4500

www.cfa.nhs.uk