DIAGNOSIS FRAUD – NHS BENCHMARKING REPORT
Welcome to RSM’s annual benchmarking report discussing reactive fraud referrals across the NHS during 2016.

INTRODUCTION

Now in its third year of production our report captures all the reactive fraud investigative work we have undertaken across our NHS client base and provides comparative data to help audit committees and management assess their counter fraud arrangements and benchmark themselves against their peers.

NHS Protect (soon to become NHS Counter Fraud Authority) reported that the total value of identified fraud in the NHS during 2015/2016 was £6.5m with ongoing investigations totalling an estimated value of £25m. The total amount of actual fraud however likely to be much more significant, as much still remains unreported or undetected.

The NHS sector is under constant pressure to change and evolve and it’s now more important than ever that providers and commissioners invest in an effective proactive counter fraud programme, to ensure that risks are minimised as far as possible.

Our report provides NHS organisations with a high-level overview on the fraud risks currently facing the sector. We discuss the key types of investigations we have undertaken across our client base and highlight which frauds have increased and new and emerging risk areas.

We’ve seen an 18 per cent increase in the number of referrals relating to suspected fraud during 2016. While this can be interpreted in a number of ways, what is clear is that fraud remains a real issue and a significant risk for the sector.

Tim Merritt
Partner, Fraud Risk Services and Head of NHS Sector at RSM

The report is based on information obtained through our internal case management system during 2016. We provide counter fraud services to 80 NHS clients nationally.

The comparative data used to create this report is based on referrals received across our NHS client base. Annual changes to the number of health bodies covered has not been analysed for the purposes of this paper.
15% of all referrals received during 2016 related to fraud where employees had undertaken unauthorised work whilst on a period of sickness absence. This remains the most common fraud type identified amongst our NHS client base and accounted for 66 referrals this year.

7% of all referrals received during 2016 related to fraud involving falsified identities. We have seen an increase from 16 cases in 2014 to 30 in 2016 and this continues to be one of the most frequently identified fraud types within our NHS client base.

11% of all referrals received during 2016 (46 cases compared to 32 in 2015) related to staff altering/falsifying timesheets. This remains the second most common fraud type identified amongst our NHS client base.

7% of all referrals received during 2016 related to fraud involving falsified identities. We have seen an increase from 16 cases in 2014 to 30 in 2016 and this continues to be one of the most frequently identified fraud types within our NHS client base.

428 referrals in 2016
£261,000 recovered for our clients
Overseas visitor offence referrals have more than doubled over the past two years.

This is now the seventh most common type of fraud referral we have seen across our NHS client base with 19 cases investigated this year compared to just seven two years ago.

The number of referrals we have seen in relation to conflicts of interest has increased from zero two years ago to 14 this year.
IS FRAUD ON THE INCREASE?

A total of 428 reactive referrals were received amongst our NHS client base during 2016. This represents an increase in total referrals from the previous year of 18 per cent and a 21 per cent increase from 2014.

The question we continue to be asked is whether fraud is actually increasing or just being reported more. The answer to both, based on our experiences and industry views, remains yes.

More fraud does appear to be happening and we firmly believe that awareness and detection has continued to improve. With the level of publicity around instances of fraud, there is less tolerance of accepting it and a reduced likelihood of ignoring it.

With the current focus on the NHS and its ongoing sustainability, there is general consensus amongst many in the sector and the general public that any fraud that takes away financial provision for patient care must not be tolerated.

Of particular note, and illustrating the ongoing development of the counter fraud provision amongst Clinical Commissioning Groups (CCGs), we have seen an increase in the number of referrals from within CCGs from 33 to 57 over the period 2015 to 2016. We believe this is a positive outcome and testament to the commitment of the sector to tackle fraud head on. This also demonstrates the benefits of focussed awareness programmes and fraud risk assessments, both of which we have undertaken with our CCG clients during 2016.

Comparative data shows us that acute trusts remain the source of the highest overall number of referrals, which is unsurprising given their size and the number of staff they employ.

NUMBER OF FRAUD REFFERALS BY ORGANISATION TYPE

- Acutes/Acute FT:
  - 2014: 6
  - 2015: 225
  - 2016: 318

- Mental Health/ MH FT:
  - 2014: 170
  - 2015: 68
  - 2016: 36

- CCG:
  - 2014: 74
  - 2015: 68
  - 2016: 57

- Community Healthcare Trust:
  - 2014: 18
  - 2015: 15
  - 2016: 1

- CIC:
  - 2014: 8
  - 2015: 7
  - 2016: 9
WHEN ARE REFERRALS MOST LIKELY TO TAKE PLACE?

During 2016 we received on average 36 referrals every month. As in previous years, we can see an increase in the number of referrals received in the month directly following our national awareness initiative, ‘fraud awareness month’, which in 2015 took place in December.

We often see an increase in referrals during or following seasonal holiday periods which may help to explain some of the fluctuations in the graph opposite. Processes and fraudulent activities can become more visible during these periods, when staff on holiday have their roles covered by temporary staff or by staff on rotation of duties. It is all too common that frauds get uncovered when those committing them are away on periods of absence from the workplace, as they are not able to sufficiently cover their tracks. Also, staff may feel more comfortable reporting concerns when their colleagues are away. 2016 saw some additional peaks in the level of referrals in the first quarter, future benchmarking exercises will determine whether or not this is a trend.

NUMBER OF FRAUD REFERRALS BY TIME OF YEAR

- June: 2016 - 44, 2015 - 14, 2014 - 44
- November: 2016 - 30, 2015 - 29, 2014 - 21

Key:
- Dark Blue: 2016
- Light Blue: 2015
- Light Green: 2014
WHERE DO REFERRALS COME FROM?

Analysing where our referrals come from gives us an understanding of how effective the awareness work undertaken by our Local Counter Fraud Specialists (LCFS) has been. This provides a basis upon which future counter fraud proactive work can be designed and undertaken.

In previous years the majority of the referrals we have received have come from existing contacts within each of our clients, specifically human resources with whom the LCFS works closely alongside in all investigations, as well as other department managers.

During 2016 we have seen an increase in the number of anonymous referrals and referrals made directly to the LCFS by members of staff. This in part may be as a result of awareness activities we undertook with our clients throughout 2016, where we educated staff on the reporting processes in place. This appears to have given staff more confidence to report their concerns directly to the LCFS, rather than via human resources or line managers.

REFERRAL SOURCES PER YEAR

<table>
<thead>
<tr>
<th>Source</th>
<th>2016</th>
<th>2015</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>General staff</td>
<td>120</td>
<td>59</td>
<td>26</td>
</tr>
<tr>
<td>Mgmt and SMT</td>
<td>73</td>
<td>82</td>
<td>87</td>
</tr>
<tr>
<td>HR</td>
<td>68</td>
<td>95</td>
<td>94</td>
</tr>
<tr>
<td>Anon</td>
<td>56</td>
<td>23</td>
<td>14</td>
</tr>
</tbody>
</table>

Key
- 2016
- 2015
- 2014
TOTAL NUMBER OF REFERRALS PER YEAR

- Fraud and corruption reporting line: 21 in 2014, 22 in 2015, 18 in 2016
- Other internal source: 5
- NHS protect: 9
- Member of public: 6
- Local security management specialist: 14

In 2014: 364
In 2015: 428
In 2016: 542
Cases of fraud related to finance have increased significantly from 58 in 2015 to 90 in 2016 with the majority of increases seen around invoice fraud and cyber security (email scams). whilst referrals received in the areas of both workforce and finance remain the largest, procurement fraud has increased significantly by 161 per cent over the past 12 months, rising from 13 referrals in 2015 to 34 in 2016. we undertook an exercise alongside a large number of our NHS clients during 2015 focusing on compliance with the NHS Standards for procurement. The effect of LCFS visibility onsite in undertaking this work, in addition to the awareness activity carried out, looks to have resulted in an increased confidence in staff reporting concerns related to procurement. We’re also seeing a greater focus within the NHS on reviewing the effectiveness of procurement functions and this increased attention may have helped to identify some fraudulent activity. we have seen little change in patient fraud related referrals over the last two years.

Working whilst sick remains the most common type of fraud referral we see in the NHS and during 2016 we have seen a significant increase in the number of referrals related to falsified identities. Most HR teams are putting stronger controls in place to identify those potential new members of staff who are using false identities and do not have the right to work. This is becoming more challenging though as the quality and authenticity of forged documents continues to improve. identifying any longstanding members of staff who may be working under a false identity is not straightforward. this remains a very real risk though for the sector as those staff would not have been subject to the same levels of scrutiny and checks when they were first employed.

Most fraud is detected by staff. Therefore, delivering a robust and targeted programme of awareness and providing staff with the knowledge and confidence to spot and report concerns is vital, as well as advising staff on their responsibilities and increasing accountability to report fraud. Encouraging staff to take ownership of where they work and NHS resources will lead to further positive changes in culture.

We have found that implementing clear reporting lines, so that staff and users can report their concerns confidentially with appropriate action taken helps accountability. This approach also acts as a deterrent to the minority who choose to defraud the health service.

WHO IS COMMITTING FRAUD?
The referrals we received in 2016 fall into four main categories:

2016

**Finance**
- 2014: 54
- 2015: 58
- 2016: 90

**Patient**
- 2014: 18
- 2015: 37
- 2016: 40

**Procurement**
- 2014: 20
- 2015: 13
- 2016: 34

**Workforce**
- 2014: 219
- 2015: 256
- 2016: 264
RECOVERIES AND SANCTIONS

Over the past year we have recovered £261,000 for our NHS clients as a result of our investigation work. We have helped achieve 85 disciplinary sanctions and 14 criminal charges have been applied. Furthermore, in seven instances we have worked jointly with external regulatory bodies to take additional action including removal from regulatory registers.

Whilst our staff focus on educating clients and assisting with the awareness and prevention of fraud, a key component of our work is to ensure our clients have robust response plans in place. These plans must enable the mobilisation of a quick and effective response to fraud incidents, to prevent further losses, secure evidence and protect the reputation and wellbeing of our clients and their staff.

A robust response plan gives an organisation a range of options to tackle fraudsters with and ensures that the benefits of the dishonest act are recovered back to the NHS where possible. Having such a mechanism also acts as a valuable deterrent tool, to deter those who give thought to defrauding the NHS.

Having a range of options in place allows for a proportionate response when determining which sanction(s) to apply, upon evaluation of the available evidence.

These are categorised as:

- criminal sanction, such as prosecution proceedings;
- internal disciplinary sanctions, to determine whether a breach of employment contract has occurred;
- regulatory sanction, where the offender is a person who falls under a professional regulator; and
- civil sanction, whereby recovery of losses and damages can be applied where appropriate, where the burden of proof is less than prosecution proceedings.

Upon conclusion of our investigations, where appropriate, we work with our clients in order to recover monies as efficiently as possible. We do this either in line with criminal sanctions or via civil recovery utilising the expert knowledge and contacts of our staff.
CASE STUDIES

FALSIFYING TIMESHEETS RESULT IN DISMISSAL

An administrations manager within a Trust worked as a substantive employee but also undertook shifts via the bank system. Investigation identified that the manager had submitted claims totalling 160 hours over a three month period for work allegedly undertaken. We identified claims in support of these hours. The employee was subject to a disciplinary hearing and dismissed from the Trust.

IT DIRECTOR JAILED FOR BRIBERY AND CORRUPTION

We undertook an investigation following concerns being raised relating to IT contracts being awarded within a hospital Trust. Our investigation identified collusion between the IT director and a contractor concerning contracts valued at £1.5m. Our investigation identified that the IT director received bribes totalling £90k, which were orchestrated by way of false invoices submitted to the Trust for payment. A subsequent referral to the police resulted in the individuals being charged with offences relating to bribery and corruption. Both individuals pleaded guilty at Crown Court to an offence of corruption. The IT director received a custodial sentence of 3.5 years imprisonment. The contractor pleaded guilty at the first opportunity and received a custodial sentence of 14 months imprisonment.

POLICE CAUTION FOR HEALTH CARE ASSISTANT WORKING WHILST SICK

Following our investigation surrounding a case of a Trust’s health care assistant working whilst sick over a four month period, we obtained sufficient evidence to prosecute the case in the criminal courts. In liaison with the police and the Trust, the Criminal Justice Office diversion from prosecution policy was applied and the subject received a police caution to record the conviction rather than proceeding through the court system.

PASSPORT FRAUDSTER IDENTIFIED AND SENT TO PRISON

An employee was investigated surrounding a suspected identity fraud. Our investigation identified that a passport, produced as part of their employment thirteen years previously, had been altered. We were engaged to review documents presented. As a result of our investigation and liaison with the Home Office the passport was established to be a forgery. The prosecution file prepared by us resulted in the subject appearing in the Crown Court, where they received a 23 week custodial sentence.

QUALIFICATIONS DECEIT RESULTS IN 12 MONTH SUSPENDED SENTENCE

We received an allegation that a health care assistant within a hospital had obtained employment through false qualifications. Following our investigation and securing the necessary evidence we obtained the support of the local police force to arrest the subject who was later charged and appeared in the Crown Court for sentencing. The hearing resulted in the subject being sentenced to 12 months imprisonment suspended for 12 month and a £3,000 fine payable to the NHS.

LOAN SHARK CAUGHT IN LCFS NET

Our LCFS received an allegation surrounding a consultant who it was alleged was operating within the Trust as an unregulated financial loans operative; ‘loan shark’. Our referral to the regulator resulted in them instigating an investigation, which led to the identification of multiple victims who had received unlawful loans in excess of £1m from the consultant. The subject was charged with offences and received a custodial sentence of 10 months imprisonment, suspended for two years, along with 120 hours unpaid work. The matter was also referred to the General Medical Council for action.
EMERGING RISKS

During the last financial year, whilst there were some new types of frauds, most are either what we define as traditional frauds, or those which are mutant versions of existing fraud types. It is for this very reason that it is vital that staff are kept appraised of ongoing fraud risks, current scams, trends and variants on fraud types that often occur.

This is where the benefits of a structured and informed awareness programme is essential, as without the knowledge, the likelihood of staff identifying fraud or having such confidence to report concerns may be lost. Most fraud is identified through staff going about their normal day to day activities in the workplace, so by not educating and empowering them, you reduce the likelihood of flushing out frauds at the earliest opportunity.

The following areas are such that we consider are likely to be continued risk areas, in addition to the traditional fraud types which we consider business as usual:

**Cyber fraud risk**

Cyber fraud risk continues to develop at a rapid pace. RSM’s latest cyber security survey highlighted that 40 per cent of organisations say they have suffered a cyber-attack, including 27 per cent that were hit in the past 12 months. Following the recent ransomware cyber-attack which affected the NHS and other organisations it is important to be alert and remain vigilant against this type of threat. Ransomware attacks are on the increase and often arrive in the form of a phishing email, spam, or some other form of nefarious email.

There are many ways that ransomware can infect your device, whether it be a link to a malicious website in an unsolicited email, or through a security vulnerability in a piece of software you use. Once the computer is infected, the ransomware will encrypt files and then demand a fee for the files to be returned. There is usually a time limit to pay up, after which the ransom increases.

We’ve also seen numerous incidents over the past 12 months whereby NHS organisations have been exposed to cyber-attacks, using methods such as hacking into systems or utilising the NHS infrastructure as a front to facilitate fraud against other organisations. In a recent case an NHS body’s server was used by an organised crime group to undertake mass email scams against members of the public.

We have also seen an increasing numbers of email request frauds, such as the CEO email scam whereby an email purporting to be from the CEO makes a request for an urgent payment to be made to a supplier. Fraudsters have stolen money from a wide number of public sector organisations using this scam.

The data held by the NHS is a valuable commodity to a fraudster. This includes supplier lists, personal data such as payroll records, and also medical records, which currently have a considerably higher black market value than credit card, bank or other personal data sets which are being traded by fraudsters.

It is critical that the threat of cyber fraud is on the board’s agenda and recognised as a strategic issue, not something that just sits with the IT department. Whilst the IT department has a role to play in securing the infrastructure, devices and patch management programmes, the risks go much wider than this. Industry experts recognise that the weak link is people. This is where educating staff on the use of organisation systems, data security, password control and use of social media is essential, if you wish to reduce your risk.

**AREAS OF FOCUS**

The NHS continues to face costs pressures and we discuss below some areas of focus we would expect organisations to consider over the coming year.

These are areas worthy of thought for proactive review and risk assessing however it is imperative that your own proactive work programme is evidence based upon a robust and thorough risk assessment process.

**Whistleblowing arrangements**

Enhancing your whistleblowing arrangements is critical to ensuring that staff have the necessary confidence and ability to report concerns. Most fraud is not detected by the LCFS or internal or external audit, but by staff within the workplace. By having an absence of, or ineffective, reporting arrangements, you increase the likelihood of fraud being perpetrated successfully, or going undetected for longer periods.

**Supply chain and contract performance**

An area which can generate positive returns in terms of assurance and redress is where you have contracts in place without robust contract management arrangements. This could be due to legacy processes, absence of corporate knowledge, such as the originator of the contract no longer being in post, through to segregation in the process where the contract delivery is never tested, either against performance, contractual terms or to the agreed original cost envelope.
There have been multiple frauds perpetrated successfully by suppliers who have leveraged contracts in their own favour, resulting in increased costs which are not in the interests of the NHS. This could involve the introduction of clauses which did not form part of original contractual terms, increase rates of pay, or decreases in volume or specification of goods or services supplied.

Recruitment
Recruitment remains a key threat and is often the gateway from which fraud can be prevented from the outset. Many organisations are now investing in technology to assist in the identification of false documents to prevent imposters or identity fraudsters gaining employment. However, there are other areas that should still be considered and reviewed, such as over reliance on technology, and the protocol in place for when systems fail or are not used correctly. We have seen cases of individuals successfully gaining employment within the NHS and then sending somebody else in their place for their induction. It’s important that the whole recruitment process is reviewed including existing staff who may have been employed prior to the enhancement of pre-employment screening processes.

Cyber fraud
Whilst organisations will continue to implement technical controls to reduce the likelihood of email scamming, some unfortunately will get through firewalls and gateways. Consequently focus should also be on training and education of staff on their responsibility for keeping data secure but also on how to respond to the ever changing threat.

THE NEXT STEPS

The financial and budgetary pressures on the NHS mean that difficult decisions must be made on a daily basis when it comes to allocating resources. Adapting your approach to tackling fraud and reviewing your proactive counter fraud initiatives is essential in helping you reduce the level of fraud occurring within your organisation.

Without this, the risk remains significant. Along with significant financial losses, fraud can negatively impact the delivery of services, damage morale of staff and reduce confidence amongst service users. The damage to your reputation could also prove irreversible.

As one of the leading external counter fraud providers in the UK, we have detailed knowledge of fraud and bribery matters within the NHS.

Our extensive team includes:

- forensic accountants;
- forensic investigators;
- certified fraud examiners;
- corporate financiers and due diligence specialists;
- insolvency specialist investigations;
- asset tracing and recovery services;
- business intelligence analysts;
- internal and external auditors;
- IT auditors;
- forensic computer e-discovery specialists;
- data analysts; and
- cyber-crime specialists.

During the coming year we’ll be introducing two new processes into our counter fraud work. These are:

- a new fraud risk assessment process. One of the outputs of this will be the production of a fraud risk register, which will highlight risks, associated controls and relevant assurances in place and any areas where controls should be further enhanced; and
- the use of data interrogation on key areas to help identify fraudulent activity eg procurement and payroll, two of the largest areas of fraud we experience.
CONTACT

For information on how we can support you, please contact Tim Merritt or your usual RSM counter fraud contact.

Tim Merritt
Partner, Forensic and Fraud Risk Services

T +44 (0)1908 687 800
tim.merritt@rsmuk.com