Temporary Staffing

Identity fraud with agency workers

See page 3

Helpful cyber advice

Cybersecurity risks are increasing

See page 4

March 2023

fraudtalk

Focus on...

Studying or attending training whilst on sick leave or special leave

When you phone your Trust to report that you are unable to attend work due to feeling unwell, most employees stay at home to recover and return to work as soon as possible… but the Counter Fraud Team are aware that some NHS staff are attending University or placements as part of their course. The team are also aware of cases where NHS staff have requested special leave and then attended University or placements. In these cases the employee will get paid by the Trust for being off sick or on special leave; this is money which they are not entitled to as they provided staff false information in order to take paid time off.

Attending University or placements whilst on sick leave or special leave is becoming an increasingly frequent referral received by the Counter Fraud Team. All bands of staff can commit this type of fraud and it is commonly found that the staff who commit this type of fraud have failed to declare they are studying outside of work to the Trust.

These investigations also raise concerns in relation to the Working Time Regulations where staff are having insufficient rest as a result of studying and working and in some cases working back to back shifts.

Here is the advice from your LCFS:

- While there may be small variations between health body policies, the main message across the NHS is that you should not be attending study, training, a course or placements whilst you are claiming sick pay from the NHS or on special leave.
- If you intend to undertake training, study or attend a course or placements whilst on sick leave or Special Leave from the NHS, you must discuss this with your line manager before you undertake the study, training, course or placements. If approved, the line manager should confirm this in writing.
- Studying, training or attending a course or placements whilst off sick or on Special Leave, can lead to disciplinary action, criminal prosecution, recovery of monies and referral to regulatory bodies such as the Nursing and Midwifery Council (NMC).
- If you have any doubts or queries regarding the Trust's rules concerning studying, training or attending a course or placement while on sick leave or special leave, contact your line manager or Human Resources Department.

fraudtalk

This edition of *FraudTalk* has been compiled by **Zenda Butler**, Head of Counter Fraud. You'll find information about local and national fraud cases as well as general advice about fraud issues.

Reminder – what to do if you suspect fraud

Do

- Report your suspicion to your LCFS immediately. If the problem is ignored, it may get worse and if it isn't addressed more money might be lost to the organisation.
- Deal with the matter promptly— the sooner it's reported the sooner the problem can be dealt with.
- Keep any evidence safe. Your LCFS will need this to form part of the case. Please don't write on it.
- Make notes on what you know/have heard or seen. It makes you more credible as a witness if you can be sure of what you're saying.

Don't

- Don't rely on someone else to make the call—the chances are they are hoping someone else will do it too.
- Don't ignore it.
- Confront any suspect yourself directly, this could give them time to destroy or remove evidence. The LCFS will notify the individual at the appropriate time.
- Start an investigation yourself. The LCFS has had specialist training to collect evidence to meet the standard required for admission in court. Any relevant findings will be shared with the health body and professional bodies so that disciplinary action can also be considered, if appropriate.
- Discuss your concerns with anyone other than the LCFS or the Director of Finance/Chief Finance Officer - you don't know whether others are involved or if they are linked to the subject.
- If you're not sure whether or not what you have found constitutes fraud or bribery or can be investigated by the LCFS, please contact your LCFS anyway. It is better that you report a concern so that we have the opportunity to decide whether we can investigate, rather than missing an opportunity to deal with suspected fraud.

ELFT's Counter Fraud Service delivers an in-house counter fraud service to East London NHS Foundation Trust (ELFT) and also provides North East London NHS Foundation Trust's (NELFT) Counter Fraud Service.

Introducing the team

Zenda Butler
Zenda is the Head of Counter Fraud at ELFT. Also the lead Local Counter Fraud Specialist (LCFS) for ELFT.

Beth Raistrick
Beth Raistrick is the LCFS responsible for all referrals relating to fraud and bribery within ELFT's Bedfordshire and Luton services.

Daniel Higgs
Daniel is the LCFS for NELFT and works across NELFT sites.

Proceeds of Crime Act 2002

The Proceeds of Crime Act or 'POCA' as it is commonly known sets out the legislative scheme for the recovery of criminal assets with criminal confiscation being the most commonly used power. Confiscation occurs after a conviction has taken place.

Proceeds of crime is the money or other assets gained by criminals whilst undertaking criminal activities and money laundering. Authorities, such as The Crown Prosecution Service, have the power to confiscate such money/assets under the Proceeds of Crime Act 2002 ("POCA").

POCA is a powerful tool that can be used and during court sentencing proceedings, a timetable can be issued to the Court which allows the Prosecuting body to ensure that confiscation can be implemented.

The legislation states 'A person benefits from criminal conduct if they obtained property as a result of, or in connection with, that conduct'; there is no specification in POCA that they had to be involved in Money Laundering offences.

One of the benefits of POCA is that investigators can apply for the original amount defrauded by the defendant and for the increase in the value of money. This is particularly beneficial for when a person has defrauded an organisation several years ago. When the matter eventually gets to court and the defendant is prosecuted and the POCA timetable is issued, there is likely to be an increase in the value of money which can be claimed.

The Local Counter Fraud Specialists (LCFS) work closely with the NHS Counter Fraud Authority's (NHSCFA) Financial Investigators (FI) in order to ensure that where criminal proceedings are pursued, there is a consideration for POCA proceedings.

Did you know your fit note can be scanned?

Statement of Fitness for Work documents, sometimes known as 'sick notes' or 'fit notes' that are produced by Healthcare professionals (usually a GP) and provided to individuals as evidence of their fitness to work, contain a QR code. This code can be scanned and will provide the person scanning it information to verify the authenticity of the document. It will show who the fit note was issued to, the name and address of the healthcare professional who issued it, and the reason the patient is signed off or alternative duties recommended. This helps verify that the fit note was in fact issued to the individual producing it as evidence of not being able to work. This type of fraud is known to occur across the NHS and is classed as Fraud by false representation, which is a criminal offence under the Fraud Act 2006, and will be investigated by the Local Counter Fraud Specialist.

Checking your Junk and Deleted emails

The Counter Fraud Team have been alerted to a case recently in relation to a successful mandate fraud at another NHS organisation. In this instance, the criminal also compromised the Chief Executive Officer's (CEO)) or CFO) email account and corresponded directly with the Finance team, diverting responses to the deleted/junk email folder where they remained unsighted by the NHS organisation's CFO.

Mandate fraud is also known as payment diversion fraud, a change of bank account scam, or supplier account takeover fraud.

By compromising the email account of the organisation's CEO, this allowed the cybercriminals to monitor the email account, intercept emails, make changes to the content of the emails, and let the emails carry on through the network. In these cases, the individual will not necessarily know their email accounts have been compromised, as emails were diverted to the junk and deleted boxes. A rule had been set up on the email account by the cybercriminal to ensure this automatically happened.

The LCFS would advise you periodically check your junk and deleted email boxes and look out for any emails you don't recognise and ones you know you hadn't sent or had sight of.

This is particularly important for staff in a position of responsibility for authorising and/or processing payments, but also a good reminder to do this for your personal and private email accounts as well.

Data matching identifies staff fraud

The National Fraud Initiative, or NFI as it is known, is the Cabinet Office's data-matching exercise which helps detect fraud and error from the public purse. NHS organisations participate in this data matching exercise every other year.

The NFI can help identify members of staff who have secondary employment at other NHS organisations or local authorities that they have not declared to their main NHS employer, in line with their trusts secondary employment, conflict of interest policy, or similar policy. It also identifies staff who have undertaken work for another NHS trust or local authority, whilst on sick leave from their substantive post.

When the NFI review for 2020 was undertaken at ELFT, four investigations commenced as a result where it was identified that staff may have worked for another NHS organisation whilst on sick leave from ELFT. To date these have resulted in two disciplinary sanctions, one of which was a dismissal and also the recovery of monies.

At NELFT five investigations commenced as a result of the 2020 NFI which remain ongoing.

The data matches for the 2022 NFI are due to be released soon for the counter fraud team to review.

If you have secondary employment which you have not yet declared in line with your employer's policy, please declare it immediately.

LCFS investigation into an Abuse of Position by a clinician at NELFT

Following an investigation by the LCFS at NELFT, a clinician was found to have abused their position and committed timesheet fraud by undertaking excessive Section 12 mental health assessments during their working hours, which resulted in them spending over 44 hours away from their substantive role. Action was taken to recover the monetary value of the fraud and the clinician paid the invoice in full. The individual has left their position at the Trust so no disciplinary investigation was instigated, however, as with all fraud and bribery cases, if they remained in employment with NELFT, this would have been considered. Cases are also referred to the General Medical Council (GMC).

The LCFS is aware of an investigation at a neighbouring mental health Trust where a clinician who was completing section 12 mental health assessments whilst on sick leave and during their NHS contracted hours was prosecuted, repaid monies to the Trust and received sanction from the GMC.

NELFT has a zero tolerance approach to fraud and bribery.

Temporary Staffing and the importance of not booking agency workers directly with agencies

It is really important all agency bookings are made via the Temporary Staffing Team, as per Trust procedures and managers do not go directly to agencies to book agency workers. Please do familiarise yourself with the relevant guidance and always contact the Temporary Staffing Team for advice. For out of hours emergency bookings where direct bookings are necessary, Temporary Staffing should be notified of the booking.

All agency workers must have the appropriate pre-employment checks in place and the Temporary Staffing Team must check the agency workers have the necessary compliance before they commence work with the Trust.

With direct bookings, the Temporary Staffing Team have not been afforded the opportunity to check the compliance, thus increasing patient safety risks, for example if a worker doesn't hold the qualifications or has not completed the necessary training.

If trusts are found to be employing an illegal worker who does not have the right to work in the UK, they are liable to a fine of up to £20,000 per worker, a prison sentence of up to five years, or both.

It's also vital to check the identification of agency workers when they first start working for your service, to ensure they are the same person who has gone through the pre-employment check process and are the individual with the necessary qualifications to undertake the role.

Any instances of identity fraud or false representation should be raised with the Local Counter Fraud Specialist.

For queries from NELFT staff, contact the Temporary Staffing Booking & Transformation Manager, Gillian.mead@nelft.nhs.uk

For queries from ELFT staff please email elft.agency-booking@nhs.net

Helpful advice to protect yourself against cyber risks

Cybersecurity risks and attacks are increasing exponentially due to the availability of simple hacking tools and artificial intelligence applications for unsophisticated and novice hackers. This increases the risk to the NHS Trust. Phishing attacks trying to get you to 'Click on a link' to deliver Ransomware that would paralyse our IT Systems and create Havoc and downtime to our patient services for long periods of time. Work and Home life with remote working and social media is blended for hackers and this means that you must take precautions in every aspect of your digital life. NHS Digital Departments are implementing Technology, Cyber Awareness and policies to combat against this threat but they need your help. If you think an email is suspicious or you need Cybersecurity advice, then please email the following; ELFT Cybersecurity eam elft.cyber@nhs.net NELFT IT Security Compliance Manager - hifzulrehman.shaikh@nelft.nhs.uk

Some Cybersecurity Tips for work and home

Think before you click

Beware of emails, texts or other promotions that seem suspicious or encourage you to urgently click on links. Even NHS emails can be compromised by hackers, who then send out phishing emails from their NHS account. If it looks suspicious, then please contact the cybersecurity team. Check the senders email address and do some due diligence – Would this person be sending me this genuinely, is the context of the email fitting with my role. Why do they want to make me 'Click' on a link?

Protect your email accounts with strong and separate passwords

Cyber criminals can use your email to access many of your personal and work accounts, leaving you vulnerable to identity theft and our organisation to compromised accounts. Consider using a foreign language as part of your password as Hackers use a 'English Dictionary attack' on your password, so a foreign language will make it stronger. Ask your cybersecurity team for password techniques or advice.

Do your homework

Scammers are fond of setting up fake e-commerce sites. Prior to making an online purchase, read customer reviews of the merchant from other independent sites. Make sure the website has a 'Lock' logo in the browser and ensure the website address is genuine.

Consider your payment options

If possible, use a credit card instead of a debit card because there are more consumer protections for credit cards if something goes awry.

Keep tabs on your bank and credit card statements

Continuously check your financial accounts for any unauthorised activity. Good recordkeeping goes together with managing your cybersecurity.

Use secure Wi-Fi

Shopping online using public Wi-Fi while at a coffee shop, airport or shopping centre is convenient, but it is not very secure. Avoid making online purchases via public Wi-Fi. Use VPN application to secure your data when on Wi-Fi as VPN creates a secure communication tunnel. Also, Hackers like to pretend to be legitimate with a fake Wi-Fi SSID access, by setting up a fake Wi-Fi near a coffee shop/ Shopping centre that pretends to be the establishments own Wi-Fi but really the hacker has control of the Wi-Fi SSID and access to eavesdrop and steal your data and passwords.

Enable multi-factor authentication

Create long and unique passphrases for all accounts and always enable MFA – Multi-factor Authentication for your emails or apps as this increases your security and prevents Hackers compromising your accounts, even if they have your password.

Fighting fraud: highlights of the work undertaken

NELFT since 1st April 2022

- Regular bite size videos on various fraud topics
- Multiple recommendations made to address system weaknesses.
- Multiple pro-active reviews checking controls and processes at the Trust to assist in mitigating fraud and loss occurring
- 23 referrals received
- One investigation progression with the Met Police and subjects charged with offences under the Computer Misuse Act and Money Laundering offences
- Multiple investigations on-going joint working with counter fraud services at other Trusts due to allegations of individuals working two positions, at different Trusts at the same time
- £1312.45 recovered and further recovery in progress.
- £38,216.70 fraud prevention by controls and process being in place
- £40,915.38 fraud identified to date. Other investigations are ongoing and further fraud identified figures will be quantifiable and added to this figure.
- 17 fraud and bribery presentations delivered

ELFT since 1st April 2022

- 45 referrals received
- £859 non-fraud prevention saving
- £29,218 fraud prevention saving
- £6861 recovered
- 6 internal/external disciplinary sanctions and one prosecution
- Regular bite size videos on various fraud topics
- Multiple recommendations made to address system weaknesses.
- Work to assess fraud risks across the Trust
- 24 fraud and bribery presentations delivered

Zenda Butler
07908 194 432
zenda.butler@nhs.net
Trust HQ, Finance Department,
Robert Dolan House,
9 Alie Street,
London E1 8DE

Beth Raistrick
07908 425 280
bethan.raistrick@nhs.net
9th Floor, Charter House,
Alma Street,
Luton LU1 2PJ

Daniel Higgs
07787 274066
Daniel.higgs1@nhs.net
CEME Centre – West Wing,
Marsh Way, Rainham,
RM13 8GQ