Fraud and Security Management Service

COVID-19 Fraud & Security Risks

All Clients

EMERGENCY GUIDANCE & INFORMATION - MARCH 2020

Executive Summary

The landscape in regards to crimes committed against the NHS has significantly changed in a very short period of time given the outbreak of the COVID-19 pandemic; going forward into 2020 – 2021 we will all need to be alert to the emerging threats and the impact these crimes will have across all NHS service lines.

Currently the NHS is facing one of the most difficult challenges in its history, responding to the COVID-19 pandemic by ensuring funding, supplies and services are being delivered to those most in need. Whilst we are all working hard to help patients, NHS colleagues and our families, there remains a significant minority who will take advantage of this crisis to commit crimes for personal gain. This minority can have a major impact on the already stretched NHS finances and staffing resource. We have started to receive the first crime reports concerning COVID-19 and we must protect NHS resources, now more than ever!

As the NHS turns to tackle the enormous task at hand, our adherence to the usual rules and organisational policies, systems and processes will almost certainly become more relaxed when the demands of supporting service delivery becomes increasingly under pressure. For example, with the sudden changes to working practice, staff may be absent due to illness or deployed elsewhere with inexperienced or new staff being hired and given great responsibility. These pressures will undoubtedly result in the usual checks and controls being bypassed. Controlled areas such as procurement, the supply chain, recruitment, sickness and absence management, E-Rostering and security of secure and safe environments will take second place to our focus on saving lives.

We are already reviewing all of our clients existing Fraud and Security Risk Assessments in the light of COVID-19 and the emergency measures being introduced by the government. In line with the latest NHS England / Improvement letter to NHS Executives which can be found by visiting; (https://www.england.nhs.uk/coronavirus/wp-content/uploads/sites/52/2020/03/20200317-NHS-COVID-letter-FINAL.pdf), all NHS organisations must consider their fraud resilience and business continuity plans to ensure they have due consideration to potential fraud, bribery, corruption and security risks.

Whilst our Fraud and Security Risk Assessments will assist our clients with identifying the risks, all NHS organisations are encouraged to review their risk registers, in line with their own local frameworks, and update them to reflect the current position with regards to some of the well-known fraud and

security risk areas during the national emergency. Risk registers should be further updated to consider and respond to emerging fraud and security risks coming out from the COVID-19 pandemic.

Our Local Counter Fraud Specialists (LCFS) and Local Security Management Specialists (LSMS) will ensure that all of our clients' counter fraud, bribery and corruption and security risk arrangements are robust. We will engage with clients regularly in regards to emerging risk areas. Whilst we recognise that priorities are focused on defeating the virus, fraud, violence against staff and thefts pose a real risk to valuable NHS resources. We are responsible together and must act now to mitigate these risks.

This document provides useful web-links and current information and guidance for all NHS organisations and their employees on how to spot and tackle the emerging fraud and security threats from the COVID-19 outbreak. The landscape will continue to evolve at a fast pace over the next 6-12 months and therefore our Fraud and Security Management Webpages, found at https://nhsfraudandsecurity.co.uk/news/ will be a useful resource for all of our clients to assist them in understanding and managing the risks going forward.

We are and remain committed to managing crime in the NHS.

COVID-19 Fraud and Security Risks

The following provides details of the risks that NHS organisations should consider as a matter of priority in respect of Fraud and Security.

Risk Area	Risks and Recent Reports	What we can all do
Cyber – online scams	The rise in online communication can heighten vulnerability to cyber, data security, and privacy threats. Cyber criminals will actively look to exploit these threats. Coronavirus-related fraud reports increased by 400% in March 2020. The National Fraud Intelligence Bureau (NFIB) reported a new trend in fraud related to Coronavirus, or COVID-19. Updated figures show there have been 105 reports to Action Fraud since 1 February 2020, with total losses reaching nearly £970,000. The majority of reports are related to online shopping scams where people have ordered protective face masks, hand sanitiser, and other products, which have never arrived. It is however likely that these scams will extend into the NHS working environment.	Ensure that staff are logged on when working remotely using VPNs. Staff should use NHSmail accounts, particularly when transferring sensitive data between insecure environments Staff should follow the principles as set out in our cyber fraud and scams guidance which can be found at; https://nhsfraudandsecurity.co.uk/security-information/cyber-crime/ IT functions should disseminate guidance about remote working and logging on to secure systems. Spam emails received through NHSMail should be reported via the NHSmail guidance to: spamreports@nhs.net. The guidance can be found at: https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/cybersecurityguide.pdf Additional Information on Coronavirus related cyber-attacks can be found on the National Cyber Security Centre website: at: https://www.ncsc.gov.uk/news/cyber-experts-step-criminals-exploit-coronavirus If in doubt, contact the LCFS or the IT function immediately.

Risk Area	Risks and Recent Reports	What we can all do
Cyber – Text Messages (SMS)	There has been a rise in the number of SMS scams reported across the UK using the COVID-19 pandemic as an opportunity to access individual's personal data and personal banking records. latest in a series of scams include; • SMS purporting to have been issued by HM Government, telling the recipient their movements have been monitored through their phone and they must pay a fine or face a more severe penalty, • SMS from 'GOV.UK ALERT'. This scam suggests individuals will receive fines for breaking lockdown. It reads: "It has come to our attention that you have been out of the house more than once. Due to this irresponsible behaviour, we are issuing a formal warning and a £250 fine". • SMS purporting to have been sent by a Local Authority to residents telling them they can claim £458 of coronavirus aid if they click on the link. • Fraudsters claiming, in an SMS appearing to have been issued by the HM Revenue & Customs (HMRC), targeting the self-employed in a scam circulating amid the coronavirus lockdown.	NHS organisations should review their mobile phone usage policies and procedures and provide employees (who have access to work mobile phones), with a reminder/instruction not to respond to text messages or click on links received from unknown sources. All text messages, believed to be a scam should be reported to the Fraud and Security Management Service by emailing: NHCCG.Fraud@nhs.net A screen print of the text message would assist the LCFS in monitoring the level of these scams received by NHS mobile phones across our client base.

Risk Area	Risks and Recent Reports	What we can all do
Cyber – Phishing emails & websites	Update from Hampshire Police Cyber Crime Unit (March 2020) - Cyber criminals are using COVID-19 themed phishing emails and websites to infect devices with ransomware and steal login details. Working from Home and self-isolation is causing more people to use the internet and thus increasing the probability of being a victim. The known themes are; • Fraudsters purporting to be from HMRC offering a tax refund and directing victims to a fake website to harvest their personal and financial details. The emails often display the HMRC logo making it look reasonably genuine and convincing. • Sending articles about the virus outbreak with a link to a fake company website where victims are encouraged to click to subscribe to a daily newsletter for further updates. Sending investment scheme and trading advice encouraging people to take advantage of the downturn. • Fraudsters purporting to be from a research group that mimic the Centre for Disease Control and Prevention (CDC) and World Health Organisation (WHO). They claim to provide the victim with a list of active infections in their area but to access this information the victim needs to click on a link /make a donation.	These attempts try to trick people into opening malicious attachments which could lead to fraudsters stealing personal information, email logins, passwords, and banking details. NHS organisations should ensure employees when working remotely, are logged on using VPNs and using NHS encrypted hardware. It is recommended that NHSmail accounts are used for security assurance. Personal emails should not be used for work purposes when working at home - a reminder should be issued to staff. Staff should follow the principles as set out in our cyber fraud and scams guidance which can be found at https://nhsfraudandsecurity.co.uk/security-information/cyber-crime/ IT functions should disseminate guidance about remote working and logging onto secure systems. If in doubt, contact the LCFS or the IT function immediately. Spam emails should be reported to NHSMail via spamreports@nhs.net and follow the NHSmail guidance: https://s3-eu-west-1.amazonaws.com/comms-mat/Training-Materials/Guidance/cybersecurityguide.pdf Please read and consider the current advice from the National Cyber Security Centre on 'Working From Home' at https://www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19

Risk Area	Risks and Recent Reports	What we can all do
Finance – Mandate Fraud	Whilst we have not received any local or national reports specifically in regards to payment diversion fraud, (also known as 'Mandate Fraud') and links to COVID-19, this is a high cost risk area and NHS organisations remains vulnerable. It is likely to evolve due to the COVID-19 pandemic and will occur across all sectors including the NHS. Mandate fraud occurs when someone contacts an NHS organisation with a request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier that regular payments are made to. If the organisation accepts the fraudulent request, the payments are then diverted into the criminal's bank account. The genuine supplier details are usually obtained from a range of sources including corrupt staff, publicly announced contracts and online logs of supplier contracts. This type of fraud can result in significant loss to the NHS and stopping these attempts relies heavily on experienced staff being trained to detect these and follow procedures. There is a risk that all mandate change requests cannot be easily verified as suppliers are under pressure and key contacts may be working remotely.	NHS organisation are encouraged to verify invoices, requests for payment and changes to supplier bank account information as far as they are able to in the circumstances The organisation should immediately review and assess their controls against the NHS Counter Fraud Authority (NHSCFA) Guidance on managing changes in bank supplier details. NHSCFA guidance can be found at: https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/quick-reference-guides/mandate-fraud.pdf In the event of identifying any concerns: • NHS organisations should Immediately report to their LCFS or Director of Finance/Chief Finance Officer • The NHS organisation should contact their targeted bank advising them of the suspected mandate fraud in action. • The NHS organisations bank should be instructed to contact the bank of the suspect account where the fraudulent transfer of NHS funds has been made to. • An immediate freeze on the funds should be requested. Reporting incidents of mandate fraud, even unsuccessful ones, will assist in the identification of individuals who are targeting the NHS and their methods for investigative action.

Risk Area	Risks and Recent Reports	What we can all do
Procurement	There is already a higher demand and desire to procure equipment quickly which can lead to compliance with procurement processes being bypassed. The emerging risks are: • Urgency to procure goods and services reduces time to complete adequate due diligence • Shortage of supply may require NHS organisations to engage with different and off framework suppliers • Controls around single tender waiver, SFI's and contract extension activity may be relaxed	Finance and procurement teams must ensure they remain vigilant to fraud risks. Employees working in these areas are encouraged to read and familiarise themselves with the NHSCFA fraud prevention advice on pre-contract procurement fraud and corruption which highlights the risks faced by NHS organisations: https://cfa.nhs.uk/resources/downloads/guidance/NHSCFA%20Pre-contract%20procurement%20fraud%20guidance%20-%20v1.0%20July%202018.pdf Due diligence should be pursued as far as is possible during COVID-19 pandemic in the time frame available; with checks continuing to progress to completion even post procurement Cumulative supplier spend should always be monitored regularly. Particular focus should be to review spend against new suppliers that have been put in place due to COVIID-19 to ensure that any new company engaged, where reduced due diligence has occurred, is not taking advantage of the current position. Where practicable put in place robust claw back agreements to be able to recover funds that are paid out incorrectly The NHSCFA have produced a short guide to buying goods and services which can be found at: https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/quick-reference-guides/buying-goods-services.pdf?v=1.0

Risk Area	Risks and Recent Reports	What we can all do
Finance – accounts payable	The Fraud and Security Management service have been alerted to the fact that some NHS organisation will be streamlining accounts payable processes to ensure prompt and advance payments for urgently required goods and services. Government advice during the COVID-19 pandemic is to maintain supplier payments irrespective of performance. This however can lead to: • Urgent payment requests that exploit COVID–19 leading to errors and duplicate payments. • Relaxed segregation and authorisation processes allowing false or inflated invoices to be paid. Given the economy and the likelihood that some businesses will face closures it is likely that some suppliers will now be required to charge the NHS at higher costs. It is therefore imperative that any increase in spending against usual suppliers is monitored and carefully reviewed.	Finance staff, as much as possible during the COVID-19 pandemic, should continue to seek to verify invoices, requests for payment and changes to supplier bank account information. Areas of control should include: • Staff instructed to seek procurement advice when engaging with a potentially new supplier. • Finance staff communicating with colleagues to confirm receipt of goods. • Checks made by staff with clients and other individuals so that they know who they are corresponding with. • Invoices should be carefully confirmed against orders and rates agreed specifically in the crisis. • Goods receipts should be confirmed prior to payment. • Supplier change requests must be confirmed using verified contact information. The NHSCFA invoice fraud guidance should be reviewed by all NHS finance staff and can be found at: https://cfa.nhs.uk/resources/downloads/guidance/NHSCFA_Invoice_and_mandate_fraud_guidance_-_v1.1_February_2019.pdf

Risk Area	Risks and Recent Reports	What we can all do
Credit cards	During the national emergency some NHS organisations may rely more heavily on credit cards to quickly secure locally required goods. As such there is a risk that: • Inappropriate purchases may not be easily identified as credit card expenditure is anticipated to temporarily increase during this period • Credit cards are likely to be used by multiple individuals due to increasing pressures. • Expenditure is reviewed retrospectively. • Non-essential or inappropriate purchases may not be promptly identified or attributed to an individual.	Records of card whereabouts should be maintained wherever possible. Itemised receipts should be retained for all credit card purchases. Statements should be reviewed and challenged promptly (where possible). The NHSCFA have produced guidance in the following documents which should be read and considered by all staff accountable and with permission to use NHS credit cards: • https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/quick-reference-guides/credit-card.pdf?v=1.0 • https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/quick-reference-guides/petty-cash.pdf?v=1.0
Theft Misappropriation	At present most of the crime reports received by the NHSCFA concern theft of medical supplies and email frauds targeting members of the public rather than the NHS specifically. However as the COVID-19 crisis ramps up, it is inevitable that there will be an urgency for NHS organisations to obtain equipment. This in turn will result in a greater volume of assets available to be misappropriated. There is a likelihood that due to the national emergency that items/stock may result in NHS stockpiling.	As far as possible, with staff resources during the crisis, stock records and asset registers should be maintained with audit trails of urgent activity retained. A local asset register should be maintained by all managers with staff working from home to ensure that all IT equipment is traceable and can be returned after the COVID-19 lockdown. This local record can be shared and checked by IT teams at the earliest opportunity. The LSMS should conduct an urgent risk assessment in high risk stock areas to determine whether additional controls would be needed during the COVID-19 pandemic.

Risk Area	Risks and Recent Reports	What we can all do
	Risks therefore include: • Relaxed controls allowing prompt movement of supplies between wards, sites and organisations. • Personal Protective Equipment (PPE), toiletries and sanitiser products could encourage and provide opportunity for individuals to steal for personal use or for black market sales. • Lack of asset tracking in regards to IT and other equipment taken by staff to work at home.	Fraud concerns should be raised immediately with the LCFS and matters relating to theft should be reported to the LSMS and local police. *(Please note – the LSMS function may be provided by the Fraud and Security Management Service or with another provider or in-house. Please check locally).
Identity theft/ Security	The Fraud and Security Management Service has received intelligence from other counter fraud sources to indicate that employees from other NHS organisations have been targeted for their identity badges. It is reported that there have been instances where staff were threatened with violence and aggression, even at knife point, for their NHS identity (ID) badges and clothing. In a time where frontline NHS employees have been acknowledged as at the forefront of dealing with COVID-19, allowing them access to shopping privileges and other rewards, there are those who will consider these items valuable. There have also been incidents across the UK where members of the public have spat at Police and other key workers and then stated that they have the coronavirus.	The NHS organisation should immediately encourage staff to wear ID at all times whilst on-site, and to actively challenge anyone who is not. Staff should however be reminded to remove their ID and, if possible, to conceal their NHS clothing and/or role prior to leaving the organisation for their own safety. Once identity has been removed staff should consider leaving buildings via public entrances to blend in unless there is no alternative. LSMS's and the police should be notified immediately if all instances occur. It is paramount that If any member of staff or patient is spat at by any person at any NHS site, that this must be immediately reported to the Police, their line manager and the LSMS. This form of behaviour during COVID-19 is now a criminal offence punishable with imprisonment.

Risk Area	Risks and Recent Reports	What we can all do
Recruitment	An increase in staffing demand due to staff sickness, self-isolation and increasing pressures will likely impact on the processing of some pre-employment screening checks. Risks include: • New applicants without the appropriate qualifications or right to work status, • Applicants with undisclosed criminal records will seek to exploit the opportunity to commence employment whilst screening is pending. • Staff in training and former staff not currently regulated will be able to join or return to the workforce. • Staff previously dismissed or convicted of fraud may find an opportunity to return to NHS workplaces and re-offend for personal gain. • References may not be sought to the usual veracity.	Pre-employment screening should be pursued to the greatest levels in the time frame available, with checks continuing to progress to completion even in instances of post recruitment. A record with a risk assessment should be made and retained where any new employees are recruited without proper due-diligence. Document scanners should be utilised wherever possible. NHS Employers have published new guidelines on each of the pre-employment check standards, to support employers to recruit quickly and safely during the COVID-19 pandemic. The new guidelines apply with immediate effect, unless otherwise specified, and relate to the recruitment of all workers and volunteers being appointed to provide emergency cover during the pandemic. The new and interim guidance can be found at: https://www.nhsemployers.org/news/2020/03/new-covid-guidelines-completing-preemployment-checks
Agency and Temporary workers	Agency staff usage will undoubtedly be increased due to employee self-isolation and increasing pressures with patients infected by COVID-19. Risks will include: • Agency staff commencing work and engagements prior to and whilst screening is pending.	Framework agencies should be utilised wherever possible, with suspected non-compliance escalated and only authorised by Executive personnel. Recruitment screening should be pursued as much as possible in the time frame available, with checks continuing to progress to completion even post recruitment Agency staff identity must be confirmed at their first shift.

Risk Area	Risks and Recent Reports	What we can all do
	• Clinical needs exceeding price caps will increase. • Some staff may inflate or falsify COVID-19 symptoms and sickness to secure paid absence from their substantive employer, in order to undertake profitable agency or bank work elsewhere	Invoices should be carefully confirmed against booking requests for hours and rates Management information in respect of staff absences should be reviewed regularly to identify staff abusing self-isolation requirements. All concerns should be reported to HR and the LCFS who will offer advice and investigate if there are grounds to do so. Staff responsible for agency recruitment and processing should be encouraged to familiarise themselves with the risks as outlined in the NHSCFA relating to agencies which can be found at: https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/Employment_agency_fraud_Guidance_on_reducing_risks.pdf?v=1.0
Payroll – Timesheet & E-Rostering fraud	Payroll processes in some NHS settings will be streamlined to ensure prompt payment. Significant increases in workforce may also complicate payroll fraud and the complex change and reimbursement arrangements may result in salary overpayments. Increased pressures will result in increased staffing costs. Physical presence and capacity due to COVID-19 will limit verification capabilities Other risks include: • Temporary staff being added to the payroll may remain on the system after the Covid-19 pandemic.	Management information should be reviewed regularly to identify multiple payroll records being paid into the same bank account (it is possible that this may be picked up later through the National Fraud Initiative Data matching). An exercise, post COVID-19, should be undertaken to check Payroll records created during COVID-19 against remaining staffing. Where possible this should be done periodically throughout the pandemic period. Timesheets and bank claims should remain under scrutiny and checking processes as far as resources allow prior to authorisation by liaising with colleagues who were physically present at the time of the

Risk Area	Risks and Recent Reports	What we can all do
	• Timesheets may be subject to limited verification due to pressures on senior clinical staff. • Ghost employees entered onto the system. • Staff may seek to gain by claiming for additional hours not worked or by failing to deduct meal breaks. • Claims may be submitted for bank claims which conflict with substantive duties, or which were not worked. • Staff failing to complete their contracted hours when working remotely and unsupervised.	shift and by using local records and knowledge. Management information should be reviewed regularly to consider the volume of hours worked by staff and to identify potential conflicts HR should provide staff and managers with guidance on remote working requirements and expected oversight/reporting. All staff responsible for payroll should familiar themselves with the risks and review the NHSCFA payroll fraud guidance document found at: https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/Payroll_fraud_guidance_March_19.pdf
Payroll – Travel and Subsistence	Whilst there is a lockdown some regular staff travel and subsistence claims may be reduced. However if the COVID-19 pandemic results in the need for non-clinical staff to be redeployed on the frontline then there could be a sharp increase in travel and subsistence expenses (as a result of staff working additional hours and across various sites). This could lead to fraudulent claims. Other risks include: • Expenses claims may be subject to limited verification in the interest of prompt payment in a period of economic crisis and personal hardship. • Claims may be made for expenses not incurred.	Staff should be reminded of the NHS organisations policies and processes with regards to claiming travel and subsistence. Guidance should be issued to all staff and updated as necessary to reflect changes to allowances and process during COVID-19. In this period of emergency and where possible this should be managed by personnel with the time to validate claims (this may require a review of trusted and authorising personnel for an interim period). Evidence of original expenditure should be always be requested and required. As far as possible accommodation should be booked centrally using arranged rates. Concerns with regards to charges over and above an agreed

Risk Area	Risks and Recent Reports	What we can all do
	• Claims for subsistence may exceed daily allowances • Accommodation costs may be required and paid for staff that need to remain away from their usual address due to redeployment or others self-isolating - Hotels may exploit the crisis by overcharging room rates or incidentals. • Staff may exceed the permitted allowances in meal / incidental charges. • Abuse of out-of-hours claims when staff are working unsupervised and remotely.	threshold for subsistence should be referred to the LCFS for further validation and investigation. The NHSCFA provides guidance for Payroll staff which can be reviewed at: https://cfa.nhs.uk/resources/downloads/guidance/fraud-awareness/Payroll_fraud_guidance_March_19.pdf
False insurance and liability claims	A significant number of NHS staff will be working from home in line with HM Government COVID-19 directions. In most instances this was done at short notice leading to staff not having the appropriate equipment and workspace areas. In addition we are receiving reports that there are inadequate stocks of PPE for staff on the frontline. There are some risks relating to insurance and liability claims against the NHS such as: • Staff may be required to work from home for a prolonged period leading to false or inflated claims for injury (due to usage of inappropriate home workstations) • Staff may be required to commence work prior to completion of an occupational health assessment, which	Guidance should be provided immediately to all NHS remote workers to assist them with the set-up of home workstations. There should be some form of process for staff to report concerns and request additional equipment for them to work at home safely to avoid unnecessary claims. Occupational health assessments, particularly those having just returned to work, should be pursued as promptly as possible in the circumstances. Stock control and procurement with regards to PPE should be maintained as far as possible The Health & Safety Executive (HSE) have provided guidance in regards to PPE and COVID-19 which can be found at: https://www.hse.gov.uk/toolbox/ppe.htm

Risk Area	Risks and Recent Reports	What we can all do
	may result in false or inflated claims for injury or illness. • Potential exposure to COVID-19 due to limited availability of PPE may result in inflated or false claims.	
Overseas visitors	Whilst everyone who needs care for COVID-19 will be considered as requiring immediate and necessary treatment (which is not payable by any patient regardless of nationality); there remains some overseas patients who will seek to exploit the NHS system. Overseas visitors attending for treatment for conditions other than COVID-19 must still be identified due to pressures on the system. Risks include: • Clinical staff may not have sufficient time or opportunity with patients to identify or challenge potential overseas visitors • Overseas visitor team ability to ward walk may be inhibited due to infection control measures	Baseline questions should be pursued by admitting staff where possible during the crisis. Guidance should be provided to admitting staff to escalate patient identity issues to the overseas visitor team/LCFS promptly. NHS organisations may wish to review their own Overseas Patients policies and update as deemed appropriate. Further guidance on overseas visitors charging regulations can be found at: https://www.gov.uk/search/all?keywords=Overseas+Visitors+Charging+Regulations&order=relevance

The Fraud and Security Management Service is regularly liaising with law enforcement and public sector colleagues and is continuously monitoring reports of fraud and other crimes against the NHS. We urge Executive NHS leads to be aware of and consider the attached Government Counter Fraud Function advice on 'Fraud Control in Emergency Management: COVID-19 UK Government Guidance' which can be found at:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875844/Fraud-Control-in-Emergency-Management-COVID-19-UK-Government-Guidance.pdf

This document details imminent threats to the NHS and the various principles for effective fraud control.

Your Fraud and Security Management team is closely monitoring the fraud and security risk developments across our client base, the NHS sector and other sectors and will report further updates when intelligence and other information is received. In the meantime should you have any concerns relating to fraud, bribery, corruption and security please do not hesitate to contact your LCFS or LSMS directly.

Contact details for the Fraud and Security Management Service team can be found by visiting; https://nhsfraudandsecurity.co.uk/contact/