ANTI-FRAUD CLIENT BRIEFING

MIAA Anti-Fraud Service March 2020

PROTECTING NHS FUNDS DURING THE CORONAVIRUS CRISIS

During this period of national emergency MIAA's anti-fraud team has seen an unprecedented level of scams and frauds being targeted at both NHS organisations and its workers, as well as against wider society. These scams are taking on a variety of forms including:

- **Organised criminal cyber/email frauds**
- **Doorstep cold callers trying to exploit the elderly and vulnerable**

The overwhelming majority of organisations working with the NHS during this challenging time will do so on a professional and legitimate basis, and their contribution is valued at this time of change and uncertainty. Unfortunately, this period will also present opportunities for those with selfish, or criminal, intentions.

The Government, through the Department of Health, is pouring significant, vital, additional funds into the NHS in order to ensure emergency equipment, resources, infrastructure and personnel are in place to tackle the crisis.

Guidance issued by the NHS Chief Executive and NHS Chief Operating Officer on the 17th March included arrangements for 'Coronavirus Cost Reimbursement', covering emergency measures around contractual payments, provider reimbursement and other additional funding arrangements – from top to bottom of the NHS. Although revised financial arrangements are being put in place, the need to ensure core financial governance and accountability remains as important as ever.

The threat is two-fold. It's vital that both valuable NHS funds are not lost to criminals and that emergency equipment, resources and personnel which are to be procured through those funds are actually obtained and in place as and when intended and on time, to prevent unnecessary loss of life

Consequently, over the coming weeks, MIAA's Anti-Fraud Service will:

- Look to issue all our clients and client staff with weekly alerts (more frequently if needed) on the latest scams and frauds being attempted by those looking to exploit this crisis. This information should be of benefit at both a corporate and personal level.
- Starting with this briefing, provide specific advice and guidance on those activities which our intelligence indicates potentially are at the most significant risk of fraud and abuse at this time; and, the essential key steps to be taken to mitigate those risks.
- Maintain a senior level advice and guidance function within our team for core client personnel in finance, procurement, workforce and staffing functions, should they have specific concerns that they wish to discuss.
- Maintain an ongoing dialogue with the NHSCFA and pass on to you any further warnings or guidance from them on how valuable emergency funds can be kept out of the hands of criminals and remain focussed at front-line staff and patients. Equally, any measures we develop locally at MIAA will be shared nationally via NHSCFA for the common good.
- Remember, you can still report actual or suspected frauds, be they Coronavirus related or not, during this time via your local Anti-Fraud Specialist or the national **Fraud & Corruption Reporting Line 0800 028 4060.**

At the time of writing, considering where emergency funding is being directed, we see the most significant, material and immediate fraud risk areas as follows.

EMERGENCY PROCUREMENT (NON-PERSONNEL GOODS & SERVICES)

There is an identified risk to NHS organisations that suppliers, whether longstanding, new or fictitious companies (fraudsters) will use COVID-19 as cover to dishonestly obtain payments that they are not entitled to.

The key risk areas relate to false, inflated or duplicate invoices and/or under or non-delivery of the goods and services being procured (particularly where normal invoicing arrangements may have been suspended). These frauds (or sharp working practices) might be undertaken by legitimate (be they NHS or non-NHS) organisations or by fraudsters masquerading as genuine suppliers.

Key activities to perform should include:

- What do you know about the supplier? Are they established, or new to you / the NHS?
- If new – what appropriate due diligence checks can you undertake rapidly to confirm they're legitimate? (Companies House; Internet search; listed on NHSCFA fraud alerts? used elsewhere in the NHS?)
- If established – are contact and bank details consistent with existing records?
- The value of the intended expenditure should influence the extent of your checks.
- Is this a one-off procurement or an ongoing facility, where duplicate invoicing may be a risk?
- Any invoices should be checked for accuracy, consistency and completeness – any changes when compared with previous invoice details should be challenged before any payment is made.
- Regardless of the payment process, fundamentally, how will you be able to check that you're getting what you're paying for, avoiding under or non-delivery, or delivery of poor quality goods? Can physical verification checks upon delivery, against the order, be undertaken practically?
- Maintain use of established internal control principles wherever possible (e.g. segregation of duties) within the procurement and finance processes. A dual control procedure for authorising payments should be implemented, if possible.
- Staff should be vigilant for invoices related to office supplies as this is a known high risk area relating to all reported mandate fraud in the NHS.

N.B. However, at this time, it is suspected that there could well be an increase in false invoices making specific reference to the provision of Covid-19 emergency goods/services with the intent of pushing payments through without challenge.

For further advice, please refer to the NHS Counter Fraud Authority's fraud prevention guidance on buying goods and services, and on due diligence, by clicking here: https://cfa.nhs.uk/fraud-prevention/fraud-guidance

EMERGENCY PROCUREMENT (ADDITIONAL NHS PERSONNEL, i.e. BANK & AGENCY STAFF etc)

NHS organisations should do what they can to ensure that any additional personnel they are procuring:

(a) actually exist and are in place (not 'ghost staff');

(b) are whom they claim to be;

(c) and, are appropriately qualified/experienced for the work that's expected of them.

Where agencies are utilised, there is always the potential for false payment claims to be submitted in the assumption that reduced checks and controls will be in place during this time.

- Are the additional staff being paid for actually in post and undertaking the work required? Spot checks by managers should facilitate this.
- Are the additional staff deployed appropriately qualified for the position they are filling? Have minimum pre-employment checks been completed?
- For agencies and other personnel providers, can invoice/payment activity to be matched to shifts booked/worked?
- Are you getting what you are paying for? Are the shifts/work that you have commissioned actually being completed? If timesheets or rotas are being utilised, are these being checked?
- ID checks are paramount to confirm individuals are who they claim to be/have a right to work/and are not a threat to staff or patients. Necessary assurances should be obtained from agencies where necessary.
- Conduct local risk assessments around recruitment/appointment in accordance with the role and nature of the work to be undertaken by the relevant individuals – risk assessments for critical clinical roles should normally be more extensive than junior administrative roles, for example.

For further advice, please refer to the NHS Counter Fraud Authority's fraud prevention guidance on Employment Agency Fraud by clicking here: https://cfa.nhs.uk/fraud-prevention/fraud-guidance#employmentAgencyFraud.

Additionally, temporary guidance from NHS Employers is available at: https://www.nhsemployers.org/covid19/assurance/preemployment-checks

MANDATE FRAUDS

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. Genuine supplier details are usually obtained from various sources including corrupt staff, publicly announced contracts and online logs of supplier contracts.

- If there should be a need to amend bank account details, suppliers should be sent a bank account amendment form for their finance director or company secretary to sign, confirming the change of bank account details. Information provided on the amendment form should be checked against the health body's existing records before any change is made.

- A senior member of the finance team should always review any change of bank account details and formally authorise this.

- All staff should be aware of and adhere to internal procedures and controls to minimise the risk of losses to this type of fraud.

- There should be segregation of duties and an appropriate level of access with respect to accessing invoice processing tools in payment systems.

For further advice, please refer to the NHS Counter Fraud Authority's fraud prevention guidance on Invoice and Mandate Frauds by clicking here: https://cfa.nhs.uk/fraud-prevention/fraud-guidance#invoiceMandateFraud

The UK Government Counter Fraud Function has also just published **Fraud Control in Emergency Management: COVID-19 UK Government Guidance**. This is useful summary information for your awareness and we are providing the guidance to you separately, alongside this briefing. It can also be found here: https://www.gov.uk/government/publications/fraud-control-in-emergency-management-covid-19-uk-government-guide

We will continue to provide, on an ongoing basis, further and/or updated guidance on primary fraud risks facing the NHS and its staff during the crisis. If you feel there's any area of NHS funding which is particularly vulnerable at this time, let us know! You can contact us directly via the details provided.

Darrell Davies
Assistant Director (Anti-Fraud)
0151 285 4520
07785 286381
darrell.davies@miaa.nhs.uk

Claire Smallman
Senior Anti-Fraud Manager
0151 285 4770
07769 304145
Claire.smallman@miaa.nhs.uk

Paul Bell
Senior Anti-Fraud Manager
0151 285 4500
07552 253068
paul.bell@miaa.nhs.uk
paul.bell2@nhs.net

MIAA
IMPROVE THE OUTCOME