MIAA 2023/2024 Insight Series

Digital Systems Fraud Prevention through Transactional Monitoring

October 2023

miaa

Introduction and Background

"Healthcare expenditure in 2021 was estimated at £227bn, which was an increase in nominal terms of 7.4% on spending in 2020. The NHSCFA has assessed, that, in the context of a 2021 to 2022 NHS budget in England of almost £150,614bn, that the NHS is vulnerable to fraud, bribery and corruption to an estimated £1.198bn.

There are more than 1.2 million full-time equivalent staff working in the NHS across 219 trusts (including 10 ambulance trusts), as well as 42 regionally based Integrated Care Systems. The NHS also has a developing relationship with private sector health providers. It is a complex landscape to operate in and means that the development of a shared strategy and a shared understanding of risk is challenging …

our strategy is a collaborative approach…

… underpinning the strategy is a desire to maximise the use of data and data techniques… whilst respecting the inherent requirements of privacy and security."

The NHS Counter Fraud Authority (NHSCFA) – 2023-26 Strategy

NHS organisations need to understand their exposure to fraud risks and should assess themselves to understand their level of fraud risk vulnerability. This assessment should include the risks posed by Digital systems.

The NHS Data Security and Protection Toolkit (DSPT) requires, under assertion 6.3.4:

- All new digital services that are attractive to cyber criminals (such as for fraud) are implementing transactional monitoring techniques from the outset.
- Completion of an assessment of which new (implemented in the last 12 months) services are susceptible to fraud and confirmation that transactional-level monitoring has been implemented to assist in the identification of potential instances of fraudulent activity.
- Transactional monitoring should be referenced in systems / services requirements documentation.

This document outlines the steps organisations should consider when implementing transactional monitoring to help prevent digital systems fraud.

Transactional Monitoring – Steps to Consider

Areas for NHS organisations to consider
• Have you reviewed the information asset register and identified systems such as finance, procurement, payroll, time activity etc. (both manual and digital systems) that may be attractive to criminals?
• Have Data Protection Impact Assessments (DPIAs) / risk assessments been performed taking into account counter fraud controls and system data flows?
• Have the following associated technical codes been reviewed: ○ Access controls ○ Sign off / authentication procedures ○ Functionality for blocking suspicious activity ○ Multi-factor authentication ○ Alerts and notifications ○ Automated controls enabled ○ Transactional monitoring capabilities ○ Transaction history integrity ○ Manual controls
• Have roles and responsibilities been assigned for the sign off / monitoring / escalation of incidents, etc. and policy / procedures documented and published?
• Has a monitoring schedule been assigned and evidenced?

Areas for NHS organisations to consider
• Are digital suppliers subject to ongoing due diligence and assurance checking e.g. associated certification / tests establishment and performance?
• Are NHS Cyber Alerts (CareCERTs) / breaches / incidents managed at an appropriate level and documented as part of the incident management plans / procedures?
• Is there clear guidance for staff, such as on the intranet / through counter fraud alerts / through training and awareness raising sessions?

Questions for Boards to Consider

Governance	Briefings
• Which roles are responsible for the system (sign-off / monitoring / escalation of incidents etc) and are they in post? • What is the governance structure to enable effective dialogue with the board to take place? • Is policy / procedure documented and published?	• When was the board last briefing on digital fraud risks?
Resilience	**Technical Controls**
• Are incidents managed at an appropriate level and documented as part of the incident management plans / procedures. • Have incident management plans / procedures for fraud incidents been reviewed / exercised?	• What authentication / sign off procedures are employed? • What authentication methods are employed to control access to the data / systems? • What access controls are in place, especially for privileged accounts? • Is transactional-level monitoring available / enabled?

• How do you collaborate with our partners / suppliers / relevant third parties, such as when undertaking investigations? • Has a monitoring schedule been assigned and evidenced as operational? • Is the supplier subject to ongoing due diligence and assurance checking? • Is data analysis being used to direct / inform prevention activity across the sector, where available?	• What assurances are there for transactional history integrity? • What alerts / notifications are there and who has access to them? • What functionality is there for blocking / reporting suspicious activity? • What controls are automated and are they enabled by default? • Is there the ability to read / archive data for an ongoing investigation? • Would you have to engage with a third party to obtain the necessary data? • Would any tools need to be purchased separately? • How do you ensure the devices / software are up to date?
Risk Management	**People**
• Have services susceptible to fraud been identified and agreed? • Has a DPIA / risk assessment been completed for each new service? • What are the plans to risk assess legacy systems? • Have system flows been mapped and counter fraud controls been documented? • Are these manual and / or digital systems?	• Do you have the right culture / capability to manage the risk? • Is there clear guidance for staff on the intranet / through counter fraud alerts / communications campaigns? • What controls / processes are manual and have they been assigned? • How experienced are your teams in fraud awareness / are there any gaps?

If you would like to discuss how MIAA can support your organisation, please contact

Paula Fagan

Head of Technology Risk

Tel: 07825 592866

Email: paula.fagan@miaa.nhs.uk

Cath Watts

Senior Technology Risk Manager

Tel: 07554 338496

Email: catherine.watts@miaa.nhs.uk