TIAN News

July 2023

Introduction

I am delighted to welcome you to our fifth edition of TIAN News. This edition spans another wide range of articles on important risk and governance issues, including:

- A checklist developed to help provide assurance over Trust's arrangements for managing Waiting Lists;
- Update regarding the new Patient Safety Incident Response Framework (PSIRF) being introduced across the NHS;
- New and increasing fraud risks arising from the development and growing use of Artificial Intelligence; and
- Key learning, and important lessons for all, arising from a major IT incident which hit Guys & St Thomas at the peak of last summer's heatwave.

Ian Wallace, Managing Director of Audit One

Waiting List Management – Assurance Checklist

The 2023/24 NHS planning guidance includes a national objective to *"reduce elective long waits and cancer backlogs and improve performance against the core diagnostic standards."* It requires all NHS healthcare providers to maximise elective activity, and expects providers to ensure ongoing clinically led review and validation of waiting lists so that patients are prioritised effectively, manage clinical risks and ensure data quality. In May, MIAA published a checklist to support NHS organisations by providing a framework for documenting and reviewing their waiting list management systems and processes. This provides an assurance mechanism over the current control framework in this area, including identifying aspects which may need strengthening.

Context:

The post-pandemic increase in waiting lists puts pressure on the systems and processes designed to manage them. Importantly, any existing process weaknesses will be exacerbated. Highly manual processes are susceptible to human error and often struggle with increases in volume. Systems that have been robust in the past may not be fit for purpose going forward.

Assurance Checklist:

The checklist sets out key challenge questions for NHS organisations to consider in each of the different areas summarised in the diagram below. These encompass the whole process - from handling of initial Referrals through to making Appointments, managing Diagnostic Tests and Communicating with Patients:

NHS organisations need to ensure that internal controls over each of these areas are robust enough to effectively manage their waiting lists within a capacity constrained system. Particular key challenges for systems and processes in this area include how they:

- Capture all patients on waiting lists?
- Effectively and consistently prioritise all patients on waiting lists and ensure the prioritisation process is clinically-led?
- Identify potential patient deterioration?
- Identify potential or actual harm caused?
- Reliably document outcomes and next steps?
- Ensure the accurate and complete transfer of patients across different waiting lists and clinicians (including when clinicians change organisations)?
- Ensure the consistent and effective management of follow up/surveillance waiting lists?
- Include accurate, complete and timely performance information reported to an appropriate group or committee?

A copy of the full Waiting List Checklist is available at www.miaa.nhs.uk/category/blog/briefings/. If you would like to discuss how internal audit can help provide assurance over this important area, then please contact your local TIAN audit lead; or for further information about this publication, please contact Louise Cobain, Executive Director of Assurance, at louise.cobain@miaa.nhs.uk / 07795 564916.

Patient Safety Incident Response Framework (PSIRF)

The longstanding Serious Incident Framework in use by all NHS bodies for managing and reporting on adverse incidents has recently been subjected to a major overhaul. The new PSIRF regime is designed to promote a proportionate approach to responding to patient safety incidents by ensuring resources allocated to learning are balanced with those needed to deliver improvement. An overview is available here: NHS England PSIRF. A preparation guide was published by NHS England in August 2022 and identifies six key phases of implementation to ease transition.

In October 2022 360 Assurance held an online workshop for clients that included presentations from the HSIB and one of the leads from an early adopter site (several NHS organisation were early adopters of the PSIRF pilot in 2020). This was a chance for patient safety leads to get together and discuss their concerns, ideas and practical initiatives in a relaxed and safe environment, as well as ask questions amongst peers. 360 Assurance received some excellent feedback, with attendees saying how useful they had found the session in helping to shape and/or consolidate their thinking about implementation.

Following on from the success of the first forum, as part of their enhanced value offer to clients this year, 360 Assurance will be running a further three workshops. The first of these will build on the forum that was held in October and will give clients an opportunity to come together to share experiences and learning from the early implementation phases. Speakers are leads from an ICB and an Ambulance Service whose organisations have both introduced novel and innovative approaches to help incorporate the requirements of PSIRF into everyday practice, making it meaningful for staff. The subsequent two sessions are likely to focus on board reporting and assurance and the LFPSE (which is the new NHSE recording system that will replace STEIS).

For more information, please contact Kristina Dickinson, Assistant Director- Clinical Quality at 360 Assurance (kristina.dickinson@nhs.net).

Artificial Intelligence – Future Fraudster?

Audit Yorkshire's counter fraud specialists have been supporting their NHS clients recently by raising awareness about the risks posed by Artificial Intelligence. The article below from Rosie Dickinson, a Local Counter Fraud Specialist within their Anti-Crime Team, summarises some of the problems arising from this new technology - and ways to protect against them.

Artificial Intelligence (AI) has the potential to make life easier – indeed many of us already use AI in our daily lives. It pops up all the time - whether it is a smart speaker telling you the weather forecast, Maps letting you know that there is heavy traffic building up on your planned route, or Spotify compiling the ultimate playlist to transport you straight back to your teenage years, AI is already embedded in our home and work environments.

Recent months have seen the development and release of more sophisticated AI tools which anyone can use, such as "Chat GPT". Greater availability of these tools brings with it many new fraud risks. For example, Chat GPT generates text at the request of the user – and what makes it unique is that it produces text with a "human tone". This makes it much harder to tell that the content has been produced by a machine.

You will almost certainly have received phishing emails that have been produced by a fraudster. Traditionally, these scam emails have had tell-tale warning signs, such as strange wording, or spelling and grammar errors that help us to spot them. The latest AI models however can create highly convincing phishing emails which are unlikely to contain spelling or grammar errors. The language it will use has been designed to sound "human". As a result, phishing emails may become much more difficult to spot. Some experts are even saying that a lack of mistakes in emails could be an indicator of a phishing email, as it may have been AI generated!

There is also new AI powered voice generating software, which can allow a fraudster to "hijack" your voice using only a 3 second clip of you speaking. A journalist has already used this software to generate clips of himself talking, and used these to log into his telephone banking (read the [full article](#) here).

Alongside these developments, there has been a rapid growth in AI art generators. These have become very popular as the user can generate impressive, bespoke profile pictures / content for use on social media. Unfortunately, some of these apps have hidden viruses lurking behind the scenes which can compromise your device and data. You may also come across AI-enabled scams on social

media sites, such as this one which was spotted on LinkedIn recently.

It is important to note that the field of AI offers many positive and exciting solutions to complex scenarios. It seems inevitable that AI will become a bigger part of our daily and working lives, so it is also important to be aware of the risk this new and emerging technology will be misused by fraudsters.
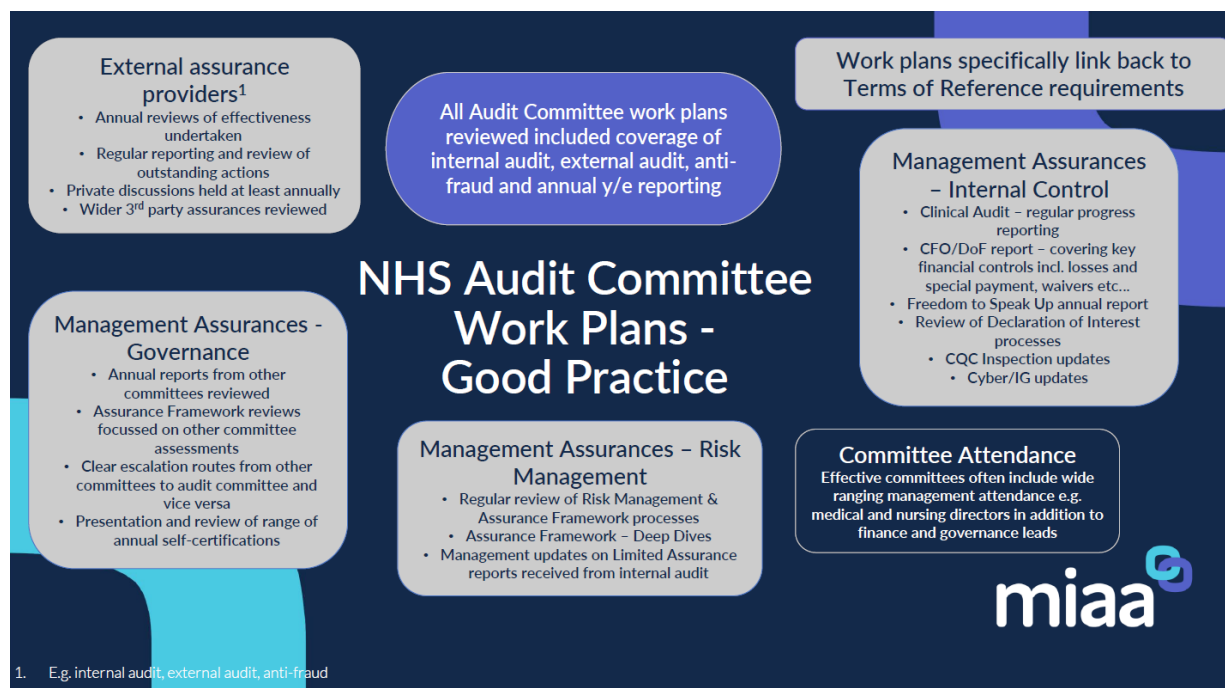
Keeping yourself safe:

- Always be suspicious if you are asked to click on a link in an email, text, or on a social media post.
- If you are on a desktop or laptop, you can use your mouse to hover over the link to see where it will take you.
- It is not easy to hover over links on touch screen devices - if in doubt, log into a desktop/laptop and hover over the link.
- With text messages which you cannot hover over, it is best to take "the long way round". For example, if you get a text apparently from your bank, do not click on any links. Instead, open a fresh web browser and manually type their address in, or use the customer service number that you'll find on the back of your bank card.
- Be wary about which apps you download – you can find some useful advice on safe app interaction on the Verified website.

If you would like to discuss the fraud risks in this area then please contact your TIAN Local Counter Fraud team.

NHS Audit Committee Workplans – Good Practice

MIAA recently issued a briefing note to support NHS Audit Committees in reviewing their coverage and programme of work through the year. Establishing an Annual Work plan for the Committee is a key tool to support its effective operation. The summary briefing (see below) highlights areas of good practice identified from a review of the plans developed by a large number of NHS Audit Committees. It is intended to support committees in reviewing their work plans and effectiveness.

If you would like further details of this study then please contact Louise Cobain, Executive Director of Assurance, at louise.cobain@miaa.nhs.uk or call her on 07795 564916.

Learning from IT Critical Incident

It is important to learn and share lessons arising from problems - which are often caused by factors facing many other NHS bodies. During the peak of the heatwave last summer, London experienced record-breaking high temperatures up to 40°C. Over the course of a day, on the 19th July, two separate data centres at Guy's Hospital and at St Thomas' Hospital both suffered failures associated with the heatwave. This took down most of the clinical IT systems at Guy's, St Thomas' and Evelina London hospitals – with the IT outage impacting 371 clinical and non-clinical IT systems.

A report to the Board of Guys & St Thomas' Trust (GSTT) earlier this year by its Deputy Chief Executive Officer sets out a comprehensive picture of the various factors leading up to the incident, as well as reviewing the Trust's response and recovery, and its impact on patients and the wider organisation. The GSTT Board committed at the outset of its review process to publishing the findings in the interests of transparency and learning - both within the Trust and beyond. This was considered important to ensure that patients, staff and partners could see a full explanation about what happened, and be assured that the Trust has undergone a searching self-reflection. Key findings from the report are summarised below.

Root cause:

- *"2.8 This review has found no single, egregious failure in the root cause analysis which has been carried out, but rather a combination of the following factors led to the catastrophic failure of the IT systems:*
    - *sub-optimal cooling systems;*
    - *ageing technological infrastructure;*
    - *overly complex and distributed roles and responsibilities for managing elements of the data centre environment; and,*
    - *partly linked to the previous point, insufficient cooling actions, both in terms of speed and scale, taken on the day of the incident to mitigate extreme ambient temperatures."*

Incident Recovery:

- *"2.5 The technical recovery of IT systems took substantially longer than was anticipated at the outset, lasting several weeks before near complete restoration. The critical site incident was stood down on 21st September, having included management of [an] unrelated cyber-attack on an external supplier from 4th August onwards."*

- *"11.4.4. The technical recovery of IT systems took substantially longer than was anticipated at the outset, lasting several weeks before near complete restoration. Part of the explanation for this protracted recovery was the multiplicity of historic IT systems - some 371 separate systems - that had been layered upon each other over time. This situation was far from best practice and the Epic system [new electronic health record system being introduced in April 2023] will consolidate and replace a large number of these legacy systems to substantially improve resilience and simplicity."*

Impact:

- *"2.9 A thorough, comprehensive and independently chaired Harm Review is examining whether any harm came to patients as a direct result of the IT outage. To date the impacts, though widespread, have been predominantly short-term delays to care and considerable inconvenience to patients. These impacts should not be under-estimated as they fall far short of the experience that the Trust and its staff expect to provide to patients. There has been one moderate harm event identified to date, and 'duty of candour' communication has been completed as a result. That no other more serious harm events have been identified after rigorous review is a clear testament to the extraordinary skill, experience and professionalism of frontline staff. It cannot, at this stage, be ruled out that further harm events may be identified, and the Trust must remain*

vigilant to this possibility as the Harm Review is completed.”

- *“2.10 It is abundantly clear … that the incident took a heavy toll on staff, who reported fatigue, stress and an adverse impact on morale. In particular, this affected frontline clinical and operational staff, who worked tirelessly to provide safe patient care, and also the IT team who worked tirelessly, often around the clock, to recover critical IT systems under immense pressure.”*

Lessons for all:

In the context of many years of constrained budgets and high operational pressures, many of the report's findings include lessons which undoubtedly apply equally to lots of other NHS bodies across the country, including:

- *“11.5.1 Extreme weather events are predicted to be more common in the future. In particular, there are predicted to be more days registering above 40°C in the future…. and more volatile, wetter winters which, [with] short, extreme cold snaps. The Trust must ensure that its digital and physical infrastructure is prepared for, and resilient to, these changing conditions.”*
- *“11.5.2 The current estate includes some specific focal points of risk, largely stemming from either ageing estate that is vulnerable to failure, or equipment that was not designed to operate in these new extreme temperatures.”*
- *“11.5.4 …a programme of staged plant and infrastructure upgrades, undertaken over the next few years, would increase overall resilience and ensure the robustness of systems to withstand the more extreme weather patterns that are likely to come”.*
- *“11.5.5 Cooling and ventilation systems should be replaced at the end of their lifespan with equipment that is designed to handle higher extreme temperature events.”*

Implications for Internal Audit:

Most internal audit plans will include periodic reviews of back up/data recovery and business continuity planning for in-house data centres. Data centre environmental controls are often given attention at initial implementation stage, ensuring that designs are consistent with best practice. The impact of climate change needs to be considered when planning reviews of temperature management/air handling/water/drug and food safety systems across the whole hospital estate.

https://www.guysandstthomas.nhs.uk/sites/default/files/2023-01/IT-critical-incident-review.pdf

For information and support regarding how internal audit can give assurance over your critical IT infrastructure risks, and robustness of associated Business Continuity Plans and Risk Management arrangements, please contact your local TIAN internal audit director. For further information about the specific issues and lessons learned at GSTT then please contact Simon Lane, Associate Director of Finance - Internal Audit Shared Service, simon.lane2@gstt.nhs.uk / 07469378265.

Data Analytics Case Study – E-Rostering

Audit Yorkshire recently used data analytics software (Arbutus) to add value to an audit of a client Trust's E-Rostering system. The aim of the review was to determine if the rostering system was being used effectively.

In the past this audit would have been completed by viewing ward rosters and testing a sample of shifts to confirm the rules built into the roster's background were being correctly applied. Using analytics however, Audit Yorkshire were able to complete testing over the whole period, and to deliver this greater level of assurance coverage in a fraction of the time.

Using reports extracted from the rostering system covering a period of six months, Audit Yorkshire were able to assess the extent to which the rostering rules were being applied. From examination of this data, the team identified a range of exceptions and challenges to rostering effectively. This included:

- Staff working more of the same shift (such as earlies or nights) in a row than permitted.
- Staff not being rostered for sufficient weekends off.
- Significantly inconsistent shift patterns in terms of start and end times - which impacts on the ability to roster effectively.
- Increased use of temporary staff (agency and bank) to cover shifts that attract a premium rate. In some cases, temporary staff filled approximately 50% of shifts overall and approximately 50% of shifts at weekends and on bank holidays.
- Additional duties had been rostered at all wards - these were duties in excess of the staffing establishment.
- All of the rosters had warnings triggered by the rules set within the system – with the average proportion of duties with warnings per roster ranging from 12% to 38%.
- 25% of staff from the wards examined owed 15 or more hours to the Trust - but had also undertaken bank work in that period.
- Reviewing booked annual leave identified issues with periods with either too many staff taking annual leave, or insufficient numbers of staff taking holidays. This can impact the ability to roster effectively as the year progresses.

These results were obtained in the context of an organisation which, like many Trusts, is struggling with a high number of vacancies. The high acuity of some patients can also impact on the need to roster additional duties. It also came to light that staff preferences are also playing a significant role in the ability to roster effectively - particularly where the organisation is keen to retain staff. The organisation is now using the audit's data analysis to explore and understand the issues identified in this review to improve its rostering practices.

Please contact your local TIAN team to find out more about how internal audit can add value to your organisation, through using data analytics to review and test whole systems and data-sets.

Events Round Up

TIAN members organise and facilitate a number of Groups and Forums across the country to support and develop NHS governance. e.g. Regional Audit Committee Chair meetings. A wide range of other education, training and networking events are also run, with many of these sessions now held virtually and being accessible to all TIAN member's NHS clients. These include:

- All Together Fairer in 2023, 13th July 2023 – This NW Collaborative Masterclass run by MIAA will explore Marmot's approach to reducing Health Inequalities.
- Procurement, 11th September 2023 - Procurement Rules are changing and will have a significant impact on NHS procurement. This half day virtual session organised by Audit Yorkshire and 360 Assurance will consider the Procurement Rules, Supply Chain Sustainability and the possibility of Mandate Fraud.
- Strengthening our sector, 15th September 2023- This NW Collaborative Masterclass run by MIAA will consider how we can harness our community assets through effective community leadership.
- Hewitt Review, 17th November 2023 – This NW Collaborative Masterclass run by MIAA will delve into how the NHS can best leverage opportunities within Integrated Care Systems
- System Working, 5th December 2023 - This half-day virtual event organised by Audit Yorkshire and 360 Assurance will consider the progress made in working across new partnerships to deliver health and social care in an equitable and sustainable way.

Watch Back: You can watch back recordings of MIAA NW Collaborative Masterclasses or read about all the previous sessions by visiting the North West Collaborative YouTube channel. Similarly, details of past events organised by Audit Yorkshire and 360 Assurance are available at https://www.360assurance.co.uk/events/ and https://www.audityorkshire.nhs.uk/events/archive-events/.

Institute of Internal Auditors Awards!

Two TIAN members were recently recognised by the IIA(UK) in their national awards for 2023. Both Barts Assurance and MIAA were finalists in the "Outstanding Team – Public Sector" category, while MIAA were also shortlisted in the "Best Innovation in Training & Development" category too! The Awards Evening held in London on 22nd June was a great event, and despite not coming away with a win it was inspiring to hear about all the exceptional work being done across the profession.

Photo, from left to right: Louise Cobain, Sarah Dowbekin and Anne-Marie Harrop from MIAA; alongside Mike Townsend and Sharon Donovan from Barts Assurance.

Find us at:

Get in touch: To find out more, or if you have feedback on any areas covered in this edition, please contact: **Mike Townsend, Managing Director of Barts Assurance | M: 07523 933348 | E: michael.townsend@nhs.net | www.bartsassurance.net | @bartsassurance**