

# TIAN News

July 2025

## Introduction

### Welcome to the Internal Audit Network Newsletter



We're pleased to bring you the latest edition of the Internal Audit Network Newsletter — your go-to source for insights, updates, and best practices in the world of internal audit. In this issue, we spotlight key developments, share thought leadership from across the network, and highlight tools and techniques that are shaping the future of audit.

Whether you're navigating regulatory changes, enhancing risk management, or driving audit innovation, we're here to keep you informed and connected.

**Louise Cobain, MIAA Executive Director of Assurance and TIAN Vice Chair**

## AI and Internal Audit: Innovation with Integrity

The digital revolution is accelerating transformation across all industries, and internal audit is no exception. Advancements in Artificial Intelligence (AI) are set to significantly reshape the way audits are conducted over the next few years. By automating data or text heavy tasks and delivering sharper insights, AI is empowering audit functions to deliver more value, faster and more efficiently. For internal audit, this is a defining moment and one that demands both innovation and vigilance.

AI enables auditors to move beyond routine checks to focus on strategic risk areas, while managing increasing demands with limited resources. For example, the Government Internal Audit Agency's 'Efficiency Engines' use AI to assess risks, generate reports, and extract insights while maintaining high standards of ethics and data security. Similarly, NHS teams are deploying AI to identify high-risk patients, speed up diagnostics, and reduce workloads—demonstrating AI's growing role in critical decision-making.

*\*\*\*\*\*However, with these advancements comes heightened responsibility\*\*\*\*\**

## A Profession at a Crossroads: Innovation and Oversight

The *Global Internal Audit Standards* stress the importance of objectivity, professional scepticism, and care. These principles are more essential than ever in the era of AI as public bodies increasingly use AI to streamline operations and reduce costs. Internal audit must not only lead in adopting AI technology, but in evaluating its impact.

Public trust must remain the priority and efficiency gains must not compromise fairness, accountability, or transparency. The Department for Work and Pensions recently faced criticism over bias in its AI fraud detection tool, which disproportionately flagged certain age and nationality groups

for fraud investigation. This underscores the need for rigorous oversight of AI systems to ensure ethical use and equitable outcomes.

### **The Internal Auditor's Dual Role**

Internal audit now has a twin mandate:

- **Innovator:** Using AI to enhance internal capabilities by automating data analysis, improving reporting, and boosting productivity.
- **Guardian:** Providing assurance over AI deployments and scrutinising algorithm design, data quality, and decision-making integrity.

To fulfil this dual role, audit teams must build confidence and capability in using and evaluating AI.

### **The Road Ahead: Actions for Internal Audit Teams**

1. **Upskill:** Train auditors in AI fundamentals, including data ethics, algorithmic bias, and emerging technology.
2. **Map the AI Environment:** Identify where AI is being used or planned. Review governance, data sources, and ethical considerations.
3. **Start Small:** Pilot AI tools in internal audit such as automating report summaries or reviewing policies against regulations.
4. **Audit AI Systems:** Extend audit scope to include AI risk. Examine models, data pipelines, and controls to ensure reliability and compliance.

### **Looking Ahead: Confidence with Caution**

Internal auditors must embrace the opportunity to lead by leveraging AI to enhance our work while ensuring its application is fair, transparent, and in the public interest. As both adopters and challengers, we must innovate with integrity. Our role is not only to use AI but to question it, govern it, and assure that it serves our highest professional values.

### **Lessons from Year One: CAF-Aligned Data Security and Protection Toolkit**

Change always gives rise to some level of uncertainty at the outset and equally the opportunity for reflection at the close. Those of us working in the health system will know this is very true for the move to the Cyber Assessment Framework-aligned Data Security and Protection Toolkit (DSPT) audit. As the audits draw to a close and the upload deadline approaches now is the time to take stock of what worked, and what didn't.

At [Audit Yorkshire](#), we're fortunate to have had the leadership of both our Deputy Director and a subject specialist to guide us through. Their work at the outset was critical to maximising the value of our audits to our clients, including through liaising with partner organisations to shortlist recommended discretionary outcomes for audit so that, for clients that chose to participate, we will be in a position to benchmark outcomes, share examples of good practice, and connect client leads in support of improving outcomes where that is wanted.

Having the workstream leadership in place, and keeping communication open, has also enabled us to apply consistent judgement against Indicators of Good Practice where there is a fine balance between the wider context of a client's approach to information security, and the specific demands of the Toolkit. That consistency has also been facilitated through our Teams chat, where colleagues undertaking Toolkit audits have shared questions and good practice as work has progressed.

The new approach to the Toolkit has also been an opportunity to further build positive relationships with clients, as they too been on that learning journey. By being able to talk through the substantial and time-pressured process, as well as how clients can improve their compliance and reduce their risk going forwards, we've been able to demonstrate that Internal Audit are supportive partners.

Now we are familiar with the new system, we know what to expect for the next round of DSPT audits. The timing of guidance being released this year was a challenge, and there was variation in the timeliness with which evidence was provided for audit. Next year, we can improve the experience by reviewing how we work with clients on those areas which are at risk of delaying the reporting process, and if any further tools can be provided to support the collation of required audit evidence.

Overall, it's been a challenging process, but thanks to the support of colleagues within Audit Yorkshire and the partnership with colleagues in the sector, a rewarding one.

Public trust must remain the priority and efficiency gains must not compromise fairness, accountability, or transparency. The Department for Work and Pensions recently faced criticism over bias in its AI fraud detection tool, which disproportionately flagged certain age and nationality groups for fraud investigation. This underscores the need for rigorous oversight of AI systems to ensure ethical use and equitable outcomes.

### **HFMA Governance Award winners**

*360 Assurance were very proud to receive the HFMA Governance Award back in December 2024 on the back of a piece of work validating GP practice lists. They worked with one ICB and Health Informatics Service to undertake the validation exercise across 127 practices, using data analytics.*

#### **Background**

As GP practices are paid a fee per patient as part of the global sum, there may be limited incentive for practices to ensure processes and controls are in place to remove patients from practice lists in a timely way, as well as pro-actively identify patients who have not had contact with the practice for some time to determine if their registration is still required.

#### **Assessing the accuracy and validity of practice size**

This piece of work assessed the accuracy and validity of practice size lists across all of the GP practices within one ICB geography (127 practices) and carried out comprehensive data analytics to detect potential 'ghost patients'.

[360 Assurance](#) worked with the local Health Informatics Service (HIS) to develop two reports for practices to run which would identify:

- A full list of all patients registered with the practice (the 'capitation report')
- A list of all patients who had not had contact with the practice in the previous three years (the 'validation report')

The HIS used various coding within the records to enable the generation of the second report. This included vaccinations/immunisations, prescriptions issued, pathology/radiology reports, community practitioner activity, clinical correspondence and registration on a Quality Outcomes Framework register as initial searches and then ran this with a couple of practices as a pilot to enable identification of other items to increase sensitivity.

Once the reports were finalised and made available through each practice's SystemOne/EMIS system, the ICB requested all practices to run these reports and securely submit them to 360 Assurance. Once all 254 reports were received, 360 Assurance carried out comprehensive data analytics on the full data set (1,202,445 patients).

### **Anomalies identified**

This identified a number of anomalies that indicated problems with the registration process and/or a lack of failsafes in the electronic patient records systems (SystemOne/EMIS):

- 732 date of birth errors (e.g. date of birth in the future or impossibly old)
- 194 patients with no NHS number
- 372 patients with no registered postcode
- 100 patients with no registered first name
- 10 patients with no registered surname
- 88 test accounts
- 1606 patients with a registration date of 31/12/1899

More concerningly, there were 4270 patients identified with the same NHS number at two different practices (something not believed was possible as it was understood there were national failsafes against this in the spine), plus 480 patients with identical demographics (name, sex, date of birth and address) but registered at two different practices with different NHS numbers and 118 patients with identical demographics registered twice at the same practice (with different NHS numbers).

Across the 127 practices there were 17,885 patients who had not received any of the contacts or interventions within three years, as picked up by the 'validation report'. Using data analytics software 360 Assurance were able to risk-assess each of these patients (based on demographics, such as age and gender) to identify those most at risk of being 'ghost patients'. The number of 'high', 'medium', 'low' and 'very low risk' patients for each practice was identified.

### **Risks of 'ghost patients'.**

There were significant numbers of patients that were at risk of being 'ghost patients'. Given the potential for fraud or simply poor use of NHS resources (and tax-payer money) where commissioners are paying for patients who might not exist, 360 Assurance worked with the ICB to put in place a prioritised programme of additional assurance and support in light of the findings.

Each practice was assigned an overall risk rating based on the data anomalies found and the number of patients at significant risk of being 'ghost patients'.

15 practices identified as high risk were provided with a detailed report of the findings relating to their practice and were required to take follow-up actions to address the discrepancies or data errors identified and provide assurance back to the ICB by a set date.

The 56 practices identified as medium risk were also provided with a detailed report of the findings relating to their practice and asked to take follow-up action.

The 56 practices identified as low risk weren't routinely provided with their specific data but were advised that there had been some minor anomalies and the PCSE guidance on registration and deregistration was provided. Positively, 15 of these practices specifically requested their data, providing assurance that they were interested in understanding the anomalies further and addressing them.

#### **Providing assurance to the ICB**

Whilst the work remains ongoing, in terms of the full benefits realisation and repeat of the detailed analysis, the process has enabled a number of deregistrations (which reduces the global sum payments by the ICB), allowed for consideration of changes to electronic systems and raised awareness with practice staff about data quality and the importance of the two-stage deregistration process, as well as providing assurance to the ICB about the governance in place within their GP practices.

Post Payment Verification (PPV) work can be undertaken on the basis of financially remedying any overclaims or underclaims by primary care services. But it can also be undertaken simply as a learning exercise for primary care services and to identify areas for improvement in systems and processes for future years. This provides assurance to commissioners about the consistency and robustness of primary care governance.

**Find out more about this work at the HFMA Governance award winner webinar – GP list validation using data analytics on 10 July, 11.30am**

To book a place on the webinar visit: [HFMA Governance award winner – GP list validation using data analytics | HFMA](#).

#### **Ethical Standards for Internal Auditors**

[Audit One](#) recently held an in-person staff training day and one of the sessions was structured around ethical standards for auditors. The session was facilitated externally by Frank Blades (Control Assurance and Training Solutions).

The session set the context of changes in IIA standards and worked through some real-life scenarios to discuss and explore the challenges facing us as auditors.

The previous Code of Ethics - Integrity, Objectivity, Confidentiality and Competence - are now covered in the Global Internal Audit Standards under Domain II Ethics and Professionalism with five standards: Demonstrate Integrity, Maintain Objectivity, Demonstrate Competency, Exercise Due Professional Care and Maintain Confidentiality

CPE remains unchanged at 40 hours annually for CIA of which 2 hours is required on ethics.

Some discussion was held on the potential tensions within the current NHS landscape; requirements for patient safety and duty of candour in the context of increasing resource constraints, workforce shortages and ageing infrastructure.

A reminder the seven Nolan principles are extant.

We discussed the definitions of:

- business ethics - *the application of ethical values such as integrity, fairness, respect and openness*
- values - *principles or standards of behaviour, inherently subjective and often uniquely held*
- culture – *often set as ‘the way things get done around here’*

Internal auditors must demonstrate integrity in their work and behaviour.

#### **Standard 1.1 Honesty and Professional Courage**

- Internal auditors must be truthful, accurate, clear, open, and respectful in all professional relationships and communications, even when expressing scepticism or offering an opposing viewpoint. Internal auditors must not make false, misleading, or deceptive statements, nor conceal or omit findings or other pertinent information from communications. Internal auditors must disclose all material facts known to them that, if not disclosed, could affect the organization’s ability to make well-informed decisions.

#### **Standard 1.2 Organisation’s Ethical Expectations**

- Internal auditors must understand, respect, meet, and contribute to the legitimate and ethical expectations of the organisation and must be able to recognise conduct that is contrary to those expectations. Internal auditors must encourage and promote an ethics-based culture in the organisation. If internal auditors identify behaviour within the organisation that is inconsistent with the organisation’s ethical expectations, they must report the concern according to applicable policies and procedures.

A scenario was discussed around an audit area with strong professional relationships in place with the client built over several years. In a pre-meet conversation, the lead states *“It’s always lovely to work with you — you understand how stretched we are. We’re hoping your report won’t make things harder with the CQC breathing down our necks.”*

Another scenario was discussed that during an audit of incident reporting and patient safety; you uncover evidence that a senior manager has been discouraging staff from reporting serious incidents to avoid triggering external scrutiny. This includes emails and meeting notes suggesting a culture of underreporting. You present your findings to the CEO, Medical Director, and Director of Nursing. The CEO, concerned about reputational damage and potential regulatory consequences, suggests “handling it internally” and delaying any formal reporting until the next quarter.

- *How would you deal with this? What do our professional standards require?*

The session finished with some discussion around the numerous types of bias we can all experience: cognitive, implicit, explicit, cultural and selection. Strategies were presented to aid more objective and fair outcomes.

In conclusion the message was - Remember we have been hired to do our job ethically and in challenging circumstances. It’s a professional requirement. But we are not alone and can always seek help and support.

The new ethical standards are summarised here with a form that can be used for a conformance return from audit staff [Tool: Ethics and Professionalism](#)

**Board Assurance Frameworks “What keeps you awake at night?”**

Review of Board Assurance Frameworks across [MIAA's](#) NHS client base for 2023/24 and 2024/25 identified a number of risk themes. This insight provides a detailed overview of the risk themes identified each year, highlights trends between the two years, and offers predictions for the rest of 2025 and beyond based on these trends. [Read more](#)

### **CAF-Aligned Data Security and Protection Toolkit (DSPT) MIAA Briefing**

The Data Security and Protection Toolkit (DSPT) has undergone a significant change for 2024-25 to align with the National Cyber Security Centre's (NCSC's) Cyber Assessment Framework (CAF). This new approach is more strategic, risk-informed, and outcome focused to drive a culture of continuous improvement in cyber security and information governance and represents a significant strengthening of requirements. [Read more](#)

### **Events Round-up**

**HFMA Governance award winner webinar – GP list validation using data analytics – Look out for the webinar in September.**

To book a place on the webinar here: [HFMA Governance award winner – GP list validation using data analytics | HFMA](#).

MIAA is a member of the [NW Collaborative hosting regular leadership Masterclasses](#). Partners are welcome to join the free Masterclasses.

**Prevention: How do we shift the focus on tackling the causes of ill health and make prevention a priority?**

**18 September**

This event will consider the government's shift within the 10 year Plan to focus on preventing ill health and the research underpinning the case for change. [Book now](#)

### **Watch Back**

You can watch back all of recordings of the NW Collaborative Masterclasses or read about all the previous sessions by visiting the [North West Collaborative YouTube channel](#).

### **Catch up with recordings of recent Masterclasses**

- Learning from [Climate Change and the Public Sector Masterclass](#)
- Learning from [Outside in Thinking Masterclass](#)
- Learning from [Collaboration in healthcare systems Masterclass](#)

### About Us:

TIAN is the collaborative network of NHS based audit and assurance providers – see [www.tian.org.uk](http://www.tian.org.uk) for further details. Together our members deliver assurance services to almost half of all NHS bodies across the country, as well as helping to support a range of other clients across the wider public sector. The member organisations comprising TIAN are:



Find us at: 

**Get in touch:** To find out more, or if you have feedback on any areas covered in this edition, please contact: **Louise Cobain, Executive Director of Assurance, MIAA** | M: 07795 564916 | E: [louise.cobain@nhs.uk](mailto:louise.cobain@nhs.uk) | [www.miaa.nhs.uk](http://www.miaa.nhs.uk) | @MIAANHS