PLACE-BASED IMPACT ACCELERATOR
DIGITAL HEALTH TECHNOLOGY

November, 2025

SECURE AI IN HEALTHCARE

Future Technology Leader Sandpit Series

Led By

Dr Rashid Kamal

The Challenge and Opportunity of AI in Healthcare

Future Technology Leader Sandpit Series

Healthcare is entering a decisive phase in its digital transformation, and developing the next generation of technology leaders is no longer optional. Our Future Technology Leader Workshops are designed to impact on academic, business and clinical leads in Belfast and beyond.

Through a twelve-session programme, we bring together emerging leaders from academia, industry, and clinical or civic organisations to share expertise, identify gaps, and generate insights that can translate into real-world impact.

Today's session examines the risks and opportunities of AI in healthcare. As organisations adopt AI-enabled tools at accelerating speed, understanding both the possibilities and the pitfalls has become a critical leadership capability.

Our next Sandpit Series workshop, planned for February/March, will explore how advances in computer vision are redefining microscopy

Stephen McComb,
Digital Healthcare Technology PBIAA Project Lead
An EPSRC Funded Project

Summary Challenge and Opportunities

"The Secure AI in Healthcare sandpit is an excellent initiative and particularly timely given the rapid adoption of AI in healthcare.

The focus on security and practical demonstrations will provide great value to the Belfast ecosystem."

Dave Vincent
Exec Lead | Northern Ireland Public Sector
Amazon Web Services

Summary Challenge and Opportunities

How do we design and deploy AI solutions in healthcare that are secure by design, resilient to malicious attack, compliant with emerging regulation, and trusted by clinicians, patients, and regulators from the device layer through to the data lake and cloud?

Scenarios

- A hospital blocks an AI model due to security concerns.
- A model's training data is poisoned, producing harmful outputs.
- Patient data leaks from IoT medical devices.
- A cyberattack delays AI deployment in a clinical setting.

Today's Agenda

01 **Welcome & Opening Remarks** – Brief introduction and overview of the session.

02 **Demonstrations** with Dr Rashid Kamal - Data Poisoning, Dr Aftab Ali - Demonstration of malware detection tools for health apps and Momentum One Zero – Product Development considerations.

03 **Panel Discussion -** Above speakers and Dr Fiona Dixon

04 **AI Perspectives** with Dr Roy Sterritt: Agentic AI, Dr Naveed Ijaz: Privacy and Confidentiality Risks of Generative AI in Healthcare and Prof Dr Zunera Jalil (Air University Pakistan): International Viewpoint

05 **Industry Experience** with Pytilla and LoughCyber

06 **Legislation & Policy Considerations** including overview of relevant legal frameworks and regulatory trends.

07 **Discussion** on the unmet needs of the group, and next steps.

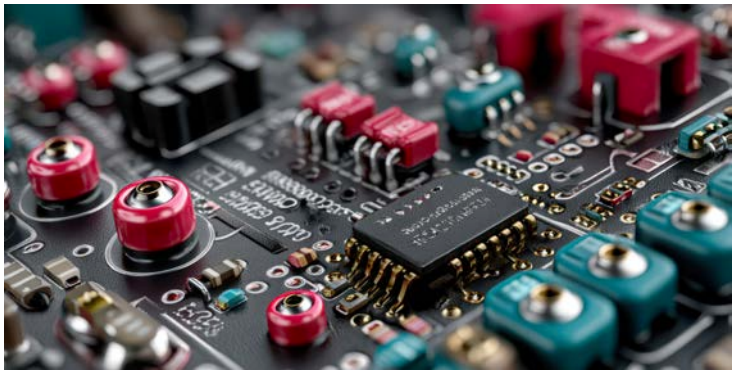
08 **Closing remarks**, key takeaways, and follow-up actions.

Demo

Today's demos are designed to move beyond traditional PowerPoint presentations, focusing instead on the practical implications of real-world implementation.

Presenters will walk us through their processes and thinking, highlighting the challenges they encounter, the tools they use, and the approaches that could inform our discussion.

This hands-on, learning-focused format is intended to spark insight, encourage questions, and provide a deeper understanding of the issues at play.



Demo 1 - Data Posioning

Invisible data poisoning is an emerging yet largely unrealised threat to healthcare, where machine-learning models and the data they depend on guide critical decisions. Even subtle, undetected distortions in training data can compromise diagnostic accuracy, skew risk predictions, and ultimately endanger patient safety. Beyond these clinical impacts, such attacks risk undermining public confidence in AI at a time when trust is vital to its effective adoption.

Dr Rashid Kamal
Researcher and Lecturer
r.kamal@ulster.ac.uk

Demo 2 - Detecting Malware in Apps

In this IoT demonstrator, Dr Aftab Ali aims to showcase urgent data-security challenges in healthcare. Demonstrating malware detection tools for health apps, including code walk-through overviews. Outlining proactively systems to safeguard patient safety and sustain trust in digital healthcare.

Dr Aftab Ali
Researcher and Lecturer

Demo 3 - Product Development

Turning healthcare ideas into functional prototypes with security built in from day one. This demo highlight how we design to protect sensor data, secure firmware and ensure trustworthy connectivity. We'll share the practical secure-by-design methods we use to ensure early prototypes are reliable, resilient, and ready to move toward clinical and regulatory pathways.

Momentum One Zero

Healthcare Voice

Healthcare faces rising challenges as AI and connected systems expand, from protecting data integrity to securing vulnerable devices. As we consider the role of AI in our healthcare, we must weigh significant concerns; patient safety, data protection, medical regulation, supplier overpromising, implementation costs, limited resources, unproven benefits, opaque decision-making, staff resistance, and the reality that we are still trying to embed more basic IT systems.

Equally, must not lose the opportunity that AI presents to address exponentially increasing healthcare demands and complex disease management.

Healthcare Voice

During the session we will have various discussions where participants are encourage to share what is working and challenging in Healthcare. Dr Fiona Dixon will participate in the panel to bring a healthcare voice to discussions.

Industry Platform

We welcome the following companies to today's session. Sharing about emerging products from their companies.

Pytilia is a fast growing technology company based in Belfast. Born from a shared vision to help organisations realise their ideas through technically excellent, united delivery teams

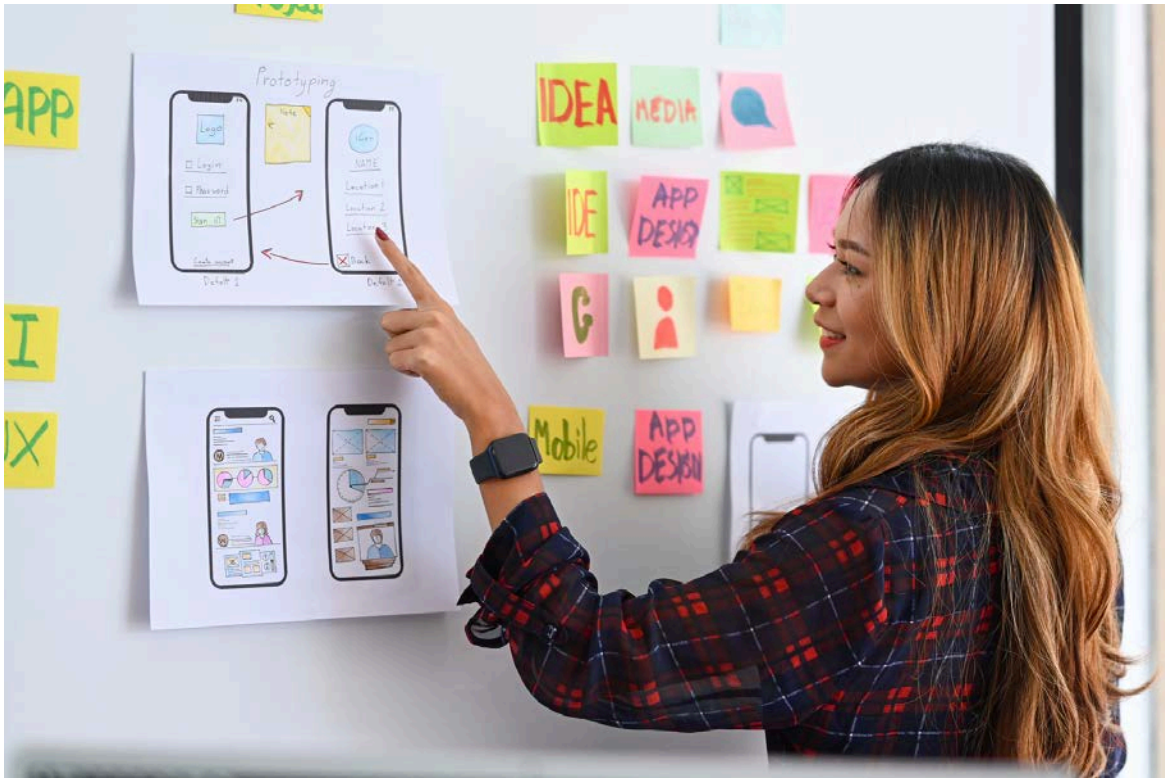
LoughTec is a trusted provider of comprehensive IT and cybersecurity solutions for businesses and organisations across Northern Ireland, the Republic of Ireland, the United Kingdom, and beyond.

Join a future session—companies can volunteer to speak and highlight their products.

Future Demonstrator

As you review the agenda, you'll notice a dedicated segment for open discussion. This is an opportunity to identify the most pressing challenges, clarify industry needs, and define actionable next steps. We are especially focused on understanding the group's unmet needs, as these will shape where meaningful innovation is most required.

In the weeks ahead, our team will translate today's insights into a practical demonstrator, designed to probe the key issues and challenges identified during this sandpit. This work will help us move from conversation to an example of what is possible.


Prototyping
IDEA
MEDIA
APP
Mobile
APP
DESIGN

Next Steps

1. Gather Challenges
2. Build a Demo
3. Present at a future webinar (approximately 4-6 weeks away)

Contact Information

Digital Healthcare Technology PBIAA

A consortium led by Ulster University has been awarded funding for an EPSRC Place Based Impact Acceleration Account (PBIAA). This is delivering tailored digital healthcare technology research and innovation activities that address the specific challenges and ambitions of Belfast and beyond. Consortium partners include Queens University Belfast, Belfast City Council and Belfast Health and Social Care Trust

Project Lead: Stephen McComb

SJ.mccomb@ulster.ac.uk

https://www.cdht.tech/

Centre for Digital Healthcare Technology

UKRI Engineering and Physical Sciences Research Council

Funding - Engineering and Physical Sciences Research Council (EPSRC)
Steering Group/Management Direction: Prof. Jim McLaughlin (UU), Prof. Adele Marshall (QUB), Prof. Chris Nugent (UU), Irwin Armstrong (CIGA Healthcare), Prof. Dewar Finlay (UU), Prof. Tim Brundle (UU), Deirdre Ferguson (BCC) and Dr Marie-Louise Cairns (EPSRC).