HEALTH AND WELLBEING

Report

Emerging Digital Technologies in Patient Care: Dealing with connected, intelligent medical device vulnerabilities and failures in the healthcare sector

PETRAS in partnership with BSI

Authors

Irina Brass, Isabel Straw, Andrew Mkwashi, Inika Charles, Amelie Soares Mesquita, Caroline Steer

UCL Department of Science, Technology, Engineering and Public Policy

Acknowledgements

We would like to extend our thanks and appreciation to all participants in the *Emerging Digital Technologies in Patient Care* workshop. We are grateful to have had such a diverse representation of practitioners and experts – clinicians and healthcare professionals, device manufacturers, standards makers, regulators, legal experts, researchers – with such deep knowledge of the healthcare sector and of the frameworks for managing medical device vulnerabilities and failures.

We are especially grateful to all the clinicians and healthcare professionals who took time out of their extraordinarily challenging jobs, especially during these very difficult times for the National Health Service (NHS) in the UK, to share their experiences of dealing with the growing use of digital technologies at the frontline of patient care.

We are equally grateful to our project partners at BSI, the UK's National Standards Body, who continue to support our Reg-MedTech project with such invaluable expertise and time. Special thanks go to Rob Turpin (Head of Healthcare Sector), Paul Sim (Medical Devices Knowledge Manager), Emma Glass (University Partnership Manager) and Matthew Chiles (Educational Development Manager).

Special thanks also go to our colleagues in the PETRAS National Centre of Excellence in IoT Systems Cybersecurity who funded the Reg-MedTech project and continue to promote our research with generous collegiality.

Last but not least, we would like to thank Dr Jesse Sowell (Lecturer in Internet Governance and Policy, UCL) for his contribution towards the development of the workshop structure and agenda in the early stages of this work.

Please cite this report as

Brass, I., Straw, I., Mkwashi, A., Charles, I., Soares, A., Steer, C. (2023) **Emerging Digital Technologies in Patient Care: Dealing with connected, intelligent medical device vulnerabilities and failures in the healthcare sector. Workshop Report**. London: PETRAS National Centre of Excellence in IoT Systems Cybersecurity. DOI: 10.5281/zenodo.8011139

Report graphics and design by Katerina Papakyriakopoulou.

About the Authors

Dr Irina Brass is an Associate Professor in Regulation, Innovation and Public Policy at UCL Department of Science, Technology, Engineering and Public Policy. She leads the PETRAS Regulation and Standardization of Connected, Intelligent Medical Devices (Reg-MedTech) project. Dr Brass specialises in the regulation of emerging technologies and the governance of responsible innovation. She has worked closely with government departments, regulatory agencies, and national and international standards-making bodies on the cybersecurity and algorithmic integrity of connected devices. Dr Brass is a member of the BSI Standards, Policy and Strategy Committee (SPSC), as well as a member and former chair of the BSI IoT-1 Technical Committee.

Dr Isabel Straw is an Emergency Doctor and a PhD Candidate in Artificial Intelligence at UCL. Dr Straw specialises in the intersection of clinical medicine, Artificial Intelligence (AI) and cybersecurity. Her previous research has exposed biases in AI systems, examined issues of tech-abuse, and evaluated models for clinical training in digital emergencies. As director of the Non-profit 'bleepDigital', Dr Straw oversees the delivery of clinical education and training events focused on cybersecurity and digital healthcare technologies. She has policy experience in both domestic and international settings, having worked on the Recommendation on the Ethics of AI and Neurotechnology at the United Nations, and as a current expert on the UK Government information Commissioner's Office (ICO) Technology Advisory Panel.

Dr Andrew Mkwashi is a Senior Research Associate – Health Innovations (Medical Devices) at Newcastle University and former Research Fellow of the PETRAS Reg-MedTech project. As an interdisciplinary researcher, he has an academic background that encompasses regulatory science, business administration, and computer science. His research interests are in the regulation, standardization and development of healthcare technologies, the governance of regulatory frameworks, the certification processes for emerging technologies, Internet of Medical Things (IoMT) cybersecurity, and exploration of artificial intelligence (AI) based medical devices, data governance and policy issues in regulatory science.

Inika Charles is a Digital Technologies and Policy MPA candidate at UCL. She holds an undergraduate degree in law and humanities, and previously worked at a law firm for four years, where she advised on technology, media and intellectual property laws in India. She is passionate about researching and advising on the regulation of technology and its impact on society.

Amelie Soares is a Digital Technologies and Policy MPA candidate at UCL. She holds an undergraduate degree in Digital Society from Maastricht University. She is passionate about interdisciplinary emerging dilemmas in digital technologies and the effectiveness of respective regulatory frameworks and initiatives.

Caroline Steer is currently studying the Digital Technology and Policy MPA at UCL. She has 10 years' experience working predominantly in technology as a business analyst, including projects for the NHS and the Health and Disability section of the Department for Work and Pensions. She is passionate about data privacy and reducing imbalances of power between Big Tech and individuals.

Contents

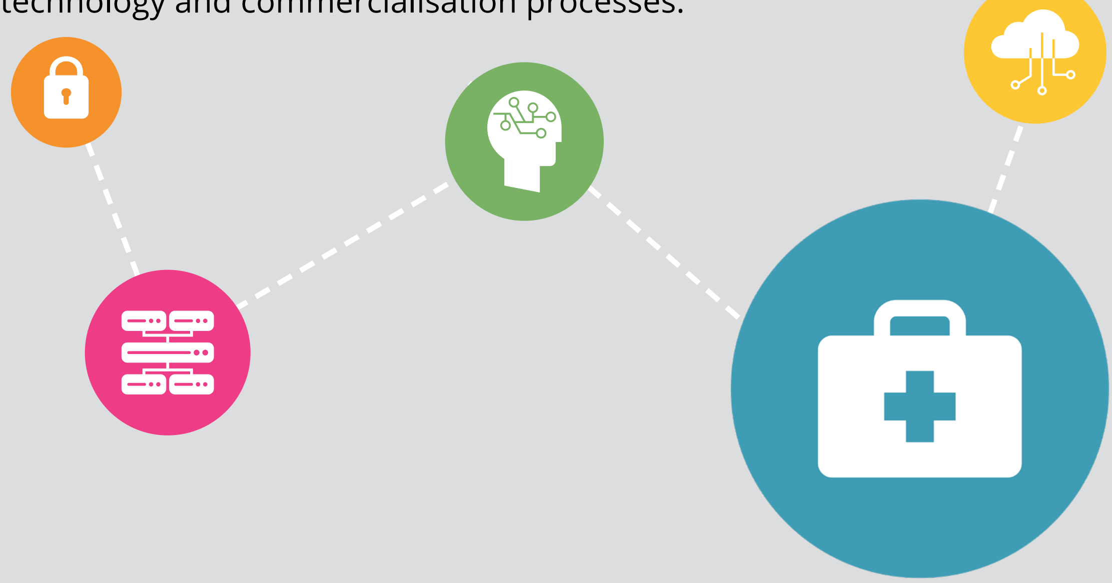
About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

To achieve our objectives, PETRAS works in collaboration with academia, industry and government partners to ensure our research can be directly applied to benefit society, business and the economy.

The Centre is a consortium of 24 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate, the University of Warwick, Keele University, and Loughborough University.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.



Executive Summary

The integration of the Internet of Medical Things (IoMT) and Artificial Intelligence (AI) into clinical routines is significantly impacting organisational preparedness at the point of care, raising concerns not only about the resilience of the healthcare infrastructure, but also about how physicians, clinicians, and healthcare professionals respond to, manage, and reduce new risks associated with connected and intelligent medical devices in the interest of patient safety and care.

The following report summarises findings from the workshop entitled *Emerging Digital Technologies in Patient Care: Dealing with Connected, Intelligent Medical Device Vulnerabilities and Failures in the Healthcare Sector*, held on 23 February 2023 at Goodenough College, London. The workshop was organised by members of the Reg-MedTech project[1], funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC grant number EP/S035362/1), in collaboration with project partners at the BSI, the UK's National Standards Body.

Since October 2021, the Reg-MedTech project has investigated the extent to which current regulatory frameworks and standards address the critical cybersecurity, data governance, and algorithmic integrity risks posed by connected and intelligent medical devices. A critical finding from its ongoing research has been the need to develop standards, regulations, and policies that are better informed by the experiences of physicians, clinicians, and healthcare professionals dealing with software-based medical devices or software as a medical device (SaMD) in their day-to-day practice.

[1] To read more about the PETRAS Reg-MedTech Project and access all its deliverables published to date, please use the following link https://petras-iot.org/project/regulatory-and-standardization-challenges-for-connected-and-intelligent-medical-devices-reg-medtech/

Workshop Aims

Through the eyes of clinicians and healthcare professionals, workshop participants were invited to share their experiences and discuss how growing cybersecurity risks and software malfunctions in connected and/ or intelligent medical devices manifest in patient care. The workshop aimed to elicit expert practitioner knowledge through real-life experiences and clinical case scenarios. Participants were invited to share, discuss, and evaluate the challenges they are facing when interfacing and interacting with various types of connected and/ or intelligent medical devices – from implantables to SaMDs – and how these experiences impact their decision-making and provision of patient care. Participants were then asked to reflect how their experiences could inform the development of future standards, guidance, and policy in the medical device field.

The workshop was attended by fifty-two participants, with representation from clinicians and healthcare professionals, public bodies including regulatory agencies, device manufacturers, legal and regulatory consultants, standards makers, and researchers.

Key Findings

We report several priority areas that have been identified and discussed through the expert and practitioner elicitation sessions during the workshop:

- **Regular training for clinicians and healthcare professionals about recurring and new cybersecurity, data quality, and algorithmic trustworthiness issues in connected and intelligent medical devices**. These issues include malware, exploits, and malicious attacks on hospital infrastructure and the IoMT, vulnerable and hackable implantables, and medical device software that could interfere with the decision-making of physicians, clinicians, and healthcare professionals in a non-transparent manner. In addition, participants identified the need for more **procedural awareness of device maintenance and reporting of possible and recognised malfunctions in hospitals and other healthcare settings**, including communications with the medical engineering teams inventorying medical devices and IT personnel in the hospital.

- **More post-market and lifecycle device management, maintenance, and support from the manufacturer**. Participants highlighted the critical need to have more support for understanding connected and intelligent medical device behaviours throughout the device's lifecycle – whether in use in hospitals or by patients – including more continuous monitoring of device performance once deployed in healthcare settings. Equally, physicians and healthcare professionals who interact with patients directly in the community – such as nurses or General Practitioners (GPs) in the UK – may need more information from manufacturers or application and digital platform owners about how medical devices such as implantables or medical apps are updated and supported throughout their lifecycle.

- **More transparent and synergetic communication between healthcare practitioners, manufacturers, and regulators about device performance and potential malfunctions**. Device specifications and capabilities, and how they interact with the patient or, in the case of SaMDs, the decisions made by practitioners in healthcare settings are not always straightforward. Often, clinicians or healthcare practitioners need to provide urgent care without knowing how implantables might interact with a patient's biological response, or how the devices they use in a hospital setting may perform if compromised or potentially compromised. Participants highlighted the critical need to have more regular communication and feedback between professional users (e.g. clinicians), end users (e.g. patients), and manufacturers to ensure all parties are kept informed of the intended use, the anticipated behaviour, and on-the-ground performance of new digital devices.

- **Responsibility and professional liability concerns**. Participants highlighted the difficulty in identifying the extent to which their clinical and professional decision-making could be affected by hacked systems or malfunctioning/ potentially malfunctioning devices. The line between product and professional liability has become thinner as a result of interactions with new software-based medical devices or SaMDs, especially AI as a Medical Device (AIaMD). The connectivity expected in hospital and healthcare settings, including the reliance on electronic medical records and cloud storage of patient records, were identified as critical vulnerability points and requiring more system resilience for the provision of reliable patient care.

1. Introduction

The Reg-MedTech project has investigated the extent to which current regulatory frameworks and standards address critical cybersecurity, data governance, and algorithmic integrity risks posed by connected and intelligent medical devices. Research conducted in the early stages of the project highlighted that the opinions and experience of clinical and healthcare practitioners could be elicited more in the development of policy, regulations, and standards pertaining to software-based medical devices or software as a medical device (SaMDs).

This is particularly relevant if we look at the structure of medical device regulations at the moment. Medical device regulations are intended for manufacturers to ensure the safety and performance of the devices they place on the market. For instance, manufacturers cannot place devices on the market without declaring the "intended purpose" and the risk classification of their device, which is then assessed by the competent authorities, such as Approved Bodies in the UK or Notified Bodies in the EU. However, through extensive expert elicitation conducted in the Reg-MedTech project, it became clear that the experience of medical device users – i.e. clinicians, physicians, healthcare professionals, and patients – needs to be better understood and captured, so that standards and regulatory guidance can address the challenges they face when directly interfacing with these devices in their day-to-day practice.

To better understand these experiences, the Reg-MedTech project organised a workshop entitled *Emerging Digital Technologies in Patient Care: Dealing with Connected, Intelligent Medical Device Vulnerabilities and Failures in the Healthcare Sector*, held on 23 February 2023 at Goodenough College, London. The workshop was structured as a practitioner and expert elicitation event and it included several practical sessions and expert talks.

In the workshop and the findings presented below, we use the following definition for a connected and/ or intelligent medical device. This definition has been developed by the Reg-MedTech project team and is not a regulatory definition.

Connected, intelligent medical devices are devices that incorporate software, including artificial intelligence, and use communication technologies and networks to transfer, manage, store, and analyse health data. These devices can be wearable or **implantable**, collect physiological patient data, and/or provide therapeutic options. They can be **software-based medical devices** or standalone **Software as a Medical Device (SaMD)**, including AI as a Medical Device (**AIaMD**). The devices themselves, the digital infrastructure that supports them, and the data collected are creating the Internet of Medical Things (IoMT) – a connected infrastructure of medical devices, software applications, and digital health systems and services[2].

1.1 Methodology

This report summarises findings from the workshop entitled *Emerging Digital Technologies in Patient Care: Dealing with Connected, Intelligent Medical Device Vulnerabilities and Failures in the Healthcare Sector*. The event was attended, in person, by several clinicians and healthcare professionals, representatives of public bodies, representatives of standards-making organizations, regulatory consultants and advisers, device manufacturers, and academics who discussed the critical challenges associated with using connected and/or intelligent devices in healthcare settings. *Figure 1* presents the total number of workshop participants by broad professional category.

Participants were invited to share their experiences and discuss how growing cybersecurity risks and software malfunctions in connected and/ or intelligent medical devices have manifested in patient care (see Annex A for the workshop agenda). The workshop used several practitioner and expert elicitation methods, including small group discussions for sharing real-life experiences and six scenarios based on documented software-based medical device malfunctions or potential malfunctions, as well as cybersecurity attacks targeting hospital setting (see Annex B for the scenarios used in the workshop.

[2] For a full discussion about the critical challenges associated with connected and intelligent medical devices, please see the Reg-MedTech White Paper entitled "The Future of Medical Device Regulation and Standards: Dealing with Critical Challenges for Connected, Intelligent Medical Devices" available at the following link https://petras-iot.org/wp-content/uploads/2021/06/White-Paper-The-Future-of-Medical-Device-Regulation-and-Standards.pdf

Stakeholder Category	Number of participants
Healthcare professionals / clinicians	20
Public body representatives	3
Device manufacturers and developers	6
Standards bodies representatives	4
Regulatory consultants / advisers	5
Academic Professionals	14
Total number of participants	**52**

Figure 1: Workshop Participants by Broad Professional Category

Workshop sessions and activities were designed with confidentiality in mind, ensuring that the workshop is a safe space for practice and experience sharing. To protect the confidentiality of participants, all workshop findings presented below are anonymised, with no direct attribution linking participants to their profession or their organisation. All event speakers have consented to their name and professional affiliation being shared in this report. The findings presented below are based on detailed note taking by the authors of this report, who formed the organisation team of the workshop.

The Reg-MedTech project has received UCL Research Ethics approval no 22137.001. The research conducted during the workshop and presented below falls under this ethics approval.

2. Clinical Cases in Digital Healthcare

The workshop opened with a presentation by **Dr Isabel Straw** entitled *Emerging Digital Technologies and Patient Care*, followed by a Q&A session and table discussions exploring the participants' own experiences of interacting with connected and/or intelligent medical devices in the healthcare setting.

In her talk, Dr Isabel Straw explored the changing landscape of health challenges that have emerged with the proliferation of digital technologies in the medical setting. The digitisation of society that has occurred over the last few decades has been paralleled by a digitisation of our bodies, minds, and experience of health and illness. Increasingly we are monitoring our wellbeing through smart apps and health platforms, we rely on the digital infrastructure of hospital systems and cloud-based telemetric care, and the prevalence of implanted medical technologies is growing at an exponential rate. While these innovative technologies bring the promise of improved diagnosis, disease monitoring, and healthcare services, their widespread adoption has also opened up our individual health, and population health, to new risks.

With each digital device we have imported into the body (e.g. pacemakers, spinal stimulators), we have potentiated a range of new clinical syndromes that may result from technological failures, electromagnetic (EM) interference, or malicious hacks. Further, as we explore novel digital environments, such as augmented and virtual reality, our physicality is interfacing with a previously unencountered technological landscape that may come with unexpected health risks.

A series of patient cases of biotechnological syndromes were provided as examples, including clinical emergencies related to malfunctioning deep brain stimulators (DBS) and cardiac arrests due to ventilator software bugs. These syndromes were described at the individual patient level (e.g., harm from hacked insulin pumps) and the population level (e.g., seizures induced by malicious hacks on twitter). As a result, the health implications of a wide range of tools were discussed, including those central to healthcare settings (e.g., drug-delivery systems), plus consumer 'wellbeing' devices. In the conclusion of the talk, Dr Straw discussed a series of ongoing research and training projects focused on raising awareness of these technological complications and improving medical education around biotechnological syndromes. In partnership with several NHS hospitals, Dr Straw's team are delivering clinical simulation sessions for healthcare professionals, in which practitioners are tasked with managing patient cases related to technology.

During the Q&A session and table discussions, participants addressed several pressing challenges when dealing with medical devices in patient care, particularly software-based medical devices and implantables. A first issue of concern is **the reporting process and feedback between clinicians, medical device manufacturers, and regulators** in the case of malfunctioning, or potentially malfunctioning, devices. It was highlighted that, while clinicians have an obligation to report device malfunctions to the regulator and/ or the manufacturer, under-reporting often occurs. This is because most hospitals do not presently have effective systems for monitoring digital healthcare technology malfunctions or these procedures are not communicated well to clinical staff. Several options to address this reporting gap were considered, including the responsibility of hospital management and trusts to train staff and to encourage reporting through clear and time-efficient instructions to clinicians and healthcare professionals. Equally, device manufacturers themselves have a responsibility to monitor their devices once on the market (known as post-market surveillance), but it was suggested this is not sufficiently and effectively done. In the case of software-based medical devices, manufacturers could and should monitor their devices more often, even in a continuous manner if possible, especially as software-based device errors are hard to identify. It was also highlighted that, in some cases, device manufacturers themselves may not be able to extrapolate what caused the malfunction or how it manifested in the device, and that some manufacturers are also reluctant to share detailed information about the malfunction or device failure due to commercial interests and confidentiality. Some participants stressed that this is a tension between the public nature of healthcare and private sector interests or broader commercial considerations, which will continue to manifest in the space of digital healthcare, especially as new data-driven technology players become more established in the sector.

A second point of discussion concerned the **professional liability** implications for clinicians providing patient care, which increasingly relies on connected or intelligent medical devices that could malfunction in ways that are not always transparent and easily identifiable. Concerns were also raised about providing care to patients with potentially malfunctioning connected or closed-loop implants (referring to a degree of automation or intelligence in the sense that the device responds to input from the patient's body). Participants raised questions about professional liability and who is responsible in cases where clinicians are uncertain about the performance of a device and are unable to reach out to manufacturers. It was also emphasised that, given the relatively sparse information that manufacturers provide to hospital staff and clinicians due to commercial confidentiality considerations, clinicians can be further disincentivised to report malfunctions that might end up questioning their professional judgement in patient care. It was highlighted that this blurs the boundaries between **professional** and **product liability** and could also show the limitations of current professional indemnity schemes. Product liability laws are currently outdated when it comes to software-based and connected products, including medical devices, and although several jurisdictions are considering updating them, it is not clear what a "software defect" could look like and how easy it will be to identify in a software-based or software as a medical device. Participants present at the workshop highlighted that the fundamental principle behind professional liability might not be affected in these cases, as long as clinicians can demonstrate that they acted in the best interest of the patient, in good faith, and utilising the best professional knowledge available to them at the time. Other participants emphasised the importance for hospitals to keep rigorous and up-to-date "medical device management systems" to ensure best practice and to minimise the risk of institutional or professional liability. The need for more substantial post-market surveillance of devices was once again highlighted as a pressing matter, this time in relation to increased professional liability concerns. For instance, some participants discussed the possibility of scanning medical devices when patients arrive with connected implantables at the hospital, which was perceived as a way of encouraging more reporting and also facilitating more transparent action about potential malfunctions and about patient decisions taken at the time of treatment.

A third issue concerned **software-based medical device lifecycle performance** and how this may differ from the lifecycle of a conventional medical device. Two instances were discussed. Participants raised concerns about the difficulty of identifying potentially compromised connected devices in the hospital setting, whose behaviour may only slowly or marginally change due to a hack, in ways that wouldn't necessarily trigger alarms. Those devices would continue to stay in use, potentially compromising patient diagnosis or treatment, as well as compromising patient data. It was also highlighted that the frequency of device monitoring (e.g., pacemakers, insulin pumps) needs to change. This points to the changing risk profile of a connected device and the limitations of current medical device risk classification frameworks. A second example pointing to software-based medical device lifecycle issues concerned the investigation of implantables post-mortem. It was highlighted that there is little clarity on whether software-based implantables are queried post-mortem (if a police investigation is not occurring) and what the procedures should be. For instance, it was mentioned that pacemakers are sent back to manufacturers post autopsy without being mentioned on death certificates. Dr Straw highlighted that she is currently working with the Coroner's Office on establishing procedures for the post-mortem investigation of such devices.

A final point of discussion concerned the **limited information available to patients** regarding their devices and the lack of training offered to clinicians to identify and query these devices as part of the diagnosis or care process. One participant discussed the challenges around device access and patient consent in clinical scenarios. They explained that when a patient was conscious, they could ask them to scan their glucose sensor with their phone and provide the reading. However, once the patient was sedated, the clinicians were no longer allowed to access the device, which sometimes impeded patient care. This highlighted the challenge of balancing **security, data protection, and access to important device data in patient care**.

3. Emerging Digital Technologies and their Evolving Challenges

The event continued with three expert talks offering different perspectives on the evolving opportunities and challenges in digital healthcare and medical device innovation:

- **Dr Richard Scott**, Director of Medical Physics & Bioengineering at University Hospitals Bristol & Weston NHS Foundation Trust, and BSI/ IEC Chair of the Electrical Equipment used in Medical Practice Committee;
- **Steven Northam**, CEO of BioTeq, a company manufacturing consumer implantable technologies;
- **Angharad Jackson**, Head of Security, Privacy and Data for the Parliamentary and Health Service Ombudsman.

In his presentation, **Dr Richard Scott** addressed the “collaborative challenges” that come up when emerging digital technologies interface with established organisational structures and processes such as those in the NHS. His talk focused on how best to minimise the risks and maximise the value from digital technologies, promoting a systematic approach that focuses on the design, adoption, and management of medical devices in a hospital setting. Dr Scott leads the medical engineering team at University Hospitals Bristol and Weston NHS Foundation Trust, where they have an inventory of over 50,000 medical devices. He highlighted the challenges associated with inventorying software as a medical device (SaMDs). His team is tasked with conducting the lifecycle management of medical devices in the hospital, including hardware, software-based medical devices, and SaMDs. He pointed out the new questions that he and his team have to consider when it comes to software-based medical devices and SaMDs, such as: “who manages the software update; what happens when the server is full; what happens when the server doesn’t have as long a lifespan as the medical device in question; if the server goes down, what is the backup plan; how long can one go without it; how many people do you give access to it”?

Dr Scott advocated that a device lifecycle management approach is critical for connected and intelligent medical devices, and that both developers and users (clinicians and healthcare professionals) should consider these questions. Dr Scott also pressed on the idea of “healthcare at the limits of science”, as mentioned in the NHS Constitution, which can be translated into a proactive and responsible way of introducing new digital technologies into the healthcare system, with appropriate design, testing, and monitoring. Dr Scott highlighted that, beyond developing medical devices for their “intended purpose” as stipulated in the regulations, we also need to think carefully about who is using it – the healthcare professionals, the patients, or the carers. Having thought-through, established device management systems in the hospital setting can help bridge this gap. Dr Scott introduced the “BRUNEL model” created with the team at University Hospitals Bristol and Weston NHS Foundation Trust. The model is a framework for the design, adoption, and management of healthcare technology. The **BRUNEL Model** consists of three ‘Tiers’:

- Tier 1 focuses on medical device design and development, taking into consideration aspects such as the purpose/ intended use of the device, and applicable risk and regulation;
- Tier 2 covers healthcare technology management and adoption, looking into business benefits, new technique training needs, and lifecycle support; and
- Tier 3 centres around value assessment, covering aspects such as strategic delivery, support, and long-term system change.

In his presentation, **Steven Northam** discussed the consumer-driven market for human microchip implants. The technology offers radio frequency identification (RFID) and near-field communication (NFC) technology and requires medical professional installation. His human microchip implant product has its own production and supply chain and comes with implant packs and hardware installation. Northam explained that the interest in this area is growing, with a particular focus on Gen Z and Gen Alpha consumers. There is a variety of use cases for microchip implants, for instance door entry systems which could benefit those with mobility issues. Other use cases include a basic data storage or payment solutions. However, there are various ethical and legal debates surrounding the technology. Northam highlighted that the consumer-driven market for human microchip implants is not regulated as strictly as the medical device sector. He acknowledged that there are concerns around consent, for instance if someone with dementia should be chipped against their will by their caretaker in order to track their whereabouts, and raised questions about who owned the chips and what happened to the data stored on them, especially after death. Northam also noted that the public perception and better understanding of use cases would be key to the success of this technology. Finally, he explained that BioTeq is exploring further developments in the R&D phases, including blood glucose level monitoring, medical data storage applications, and nano-generation and reporting.

In her presentation, **Angharad Jackson** explained the role of the Ombudsman as an impartial investigator of complaints made against the NHS and other government departments. The Ombudsman regularly investigates for maladministration in situations where, for instance, a public body has perpetuated bias or delayed delivering treatment for so long that it had an effect in injustice. She highlighted that approximately 85% of complaints received relate to healthcare issues. Jackson explained that the nature of recent complaints is changing, especially when it comes to the evidence needed to investigate cases brought to the attention of the Ombudsman. Recently, and especially since the Covid-19 pandemic, cases brought forward involve “very complex chains of interactions” requiring considerably more evidence, and sometimes evidence that can change and be lost during these interactions. This represents a challenge for the Ombudsman, who must investigate comprehensively and fairly as per its statutory duty. Jackson provided a fictitious example involving a smart insulin pump. In this case, evidence needs to be collected about interactions between patient and clinicians, community nurses, members of the family, a smartphone device, a WiFi network, a mobile cellular provider, etc.

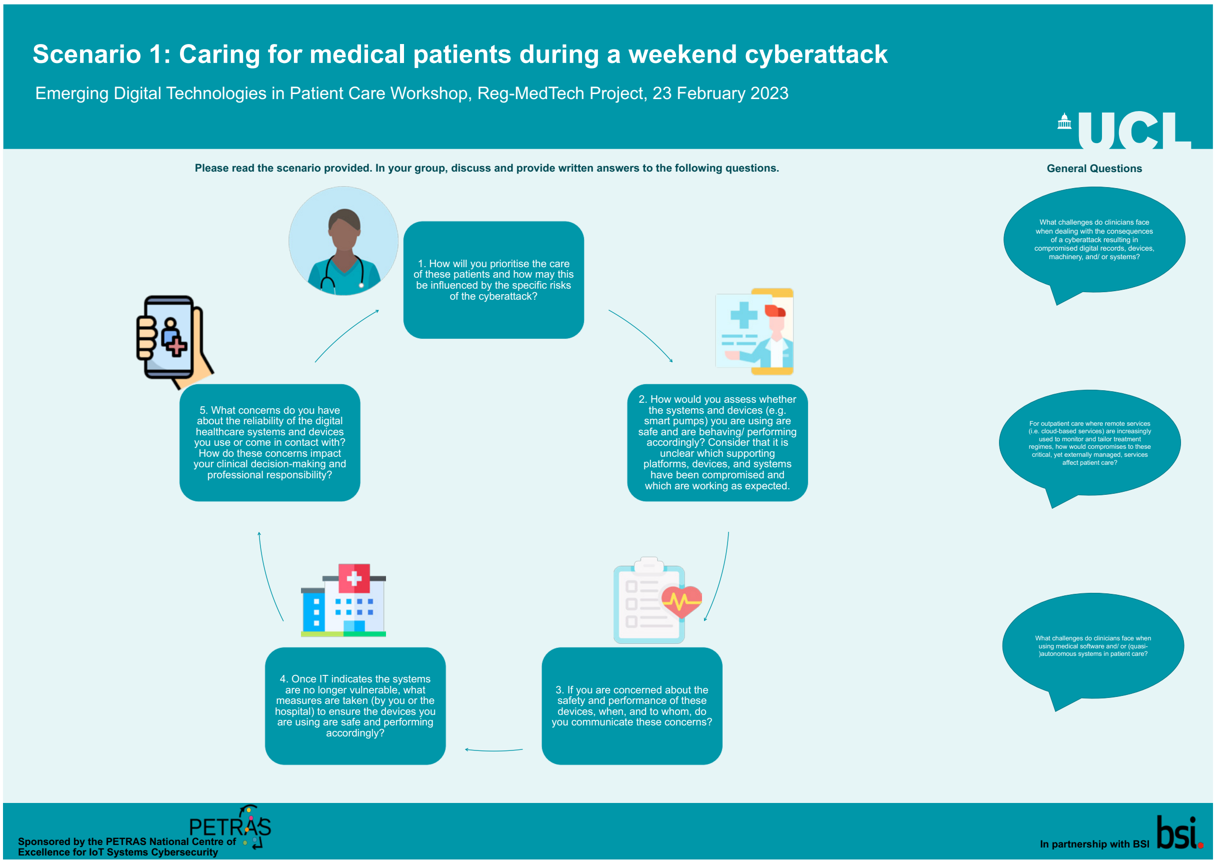
In her own words, “there are lots of different interplays and lots of different places within that increasing complexity where things could go wrong” and this is posing real challenges, especially as “the more fragmented and diverse the number of devices and digital therapeutics at play are”. Jackson provided another useful example. If someone has mental health issues, and they are receiving treatment by app (e.g., for CBT), and they complain about the treatment, can the Ombudsman recreate what the patient was prescribed if, for instance, the app was updated? Is it possible to recreate the conversation between the AI-driven chatbot and the patient at the point where the patient believes that the app no longer acted for them? Lastly, Jackson highlighted that the situation gets even more complex when we start looking at the wider population and our different experiences with and awareness of what digital technologies can do in the healthcare space. First of all, presuming digital literacy from the wider population can be a barrier to receiving appropriate attention, care, or treatment. Second, the more complex and fragmented the evidence becomes, the more need there is for trained healthcare professionals who understand how medical treatment interfaces with digital technologies, taking a “cradle to grave view” of medical devices. Jackson concluded her talk by highlighting that the Ombudsman is thinking ahead of what is to come in the digital and software-based medical device world and how they can be best equipped to deal with these challenges in the interest of the public.

4. Scenarios for Dealing with Connected, Intelligent Medical Device Vulnerabilities and Failures

The event followed with a practical session inviting participants to work in small groups on six scenarios describing compromised or potentially compromised connected and/ or intelligent medical devices. The scenarios were fictitious but based on data collected from real-life cases of medical device malfunctions and cybersecurity incidents reported in the specialist literature. The scenarios are presented in full in Annex 2 of this document, including the questions that the participants were asked to address and the literature the scenarios are based on.

Overall, each scenario asked participants to reflect on the steps, measures, and decisions they would take if placed in a situation where medical devices become compromised or are suspected to have been compromised. The questions were designed to allow participants to reflect on their awareness of the behaviour of connected and intelligent devices, which could be compromised in ways that are not always immediately clear. Also, the participants were asked to reflect on what follow-up steps they would take, including communication with other colleagues and site managers. Lastly, the participants were asked to reflect on the implications of these situations for their clinical decision-making and professional responsibility. An example of the scenario worksheet that participants had to respond to is presented in *Figure 2* below.

In the following sections, we briefly introduce each scenario and summarise the responses considered by participants in their groups. Each group included representatives from most stakeholder categories present at the workshop. Given the nature of the scenarios and questions, several clinical and healthcare professionals were present in each group. The scenarios also capture different types of situations involving medical devices in a healthcare setting: 3 medical, 1 surgical, 1 emergency, and 1 community care.



Scenario 1: Caring for medical patients during a weekend cyberattack

Emerging Digital Technologies in Patient Care Workshop, Reg-MedTech Project, 23 February 2023

Please read the scenario provided. In your group, discuss and provide written answers to the following questions.

1. How will you prioritise the care of these patients and how may this be influenced by the specific risks of the cyberattack?

2. How would you assess whether the systems and devices (e.g. smart pumps) you are using are safe and are behaving/ performing accordingly? Consider that it is unclear which supporting platforms, devices, and systems have been compromised and which are working as expected.

3. If you are concerned about the safety and performance of these devices, when, and to whom, do you communicate these concerns?

4. Once IT indicates the systems are no longer vulnerable, what measures are taken (by you or the hospital) to ensure the devices you are using are safe and performing accordingly?

5. What concerns do you have about the reliability of the digital healthcare systems and devices you use or come in contact with? How do these concerns impact your clinical decision-making and professional responsibility?

General Questions

What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?

For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

In partnership with BSI

Figure 2: Example of scenario worksheet used during the event

4.1 Scenario 1 (Medical): Caring for medical patients during a weekend cyberattack

Summary of Scenario

The group was given the task of determining an appropriate response to a healthcare cyberattack that compromised a cloud-based chemotherapy platform, drug-delivery systems, and the patient electronic medical notes. The scenario was set during on-call hours to invite discussion on the additional challenges posed by a lack of specialist staff during out-of-hours. In the scenario, the participant is positioned as a member of the general medical team, who arrives for their hospital shift to be informed that an overnight cyberattack has affected the wireless network of the hospital and all computing systems, precluding the evaluation of patients radiological and laboratory reports. The case included a description of four patients requiring immediate care, that the group had to decide how to prioritise and manage. The effective care of these patients was dependant on careful medication and fluid management, hence the security concerns regarding the drug-delivery systems and smart pumps were of paramount concern.

Discussion of Scenario

In a short time, the group determined that the event should be classed as a **Major Incident**, placing the event under the same category as fires, terrorist attacks, and chemical outbreaks. References were made to previous major events that clinicians had been involved in (e.g., Manchester bombing, Grenfell and the Hillsborough disaster). Senior clinical members of the team involved in these events identified that this **classification would initiate a chain of responses that would enable an effective co-ordinated response, such as the appointment of incident leaders, access to on-call staff and a nationally coordinated communication effort to other hospitals**. Participants reflected on the 2017 WannaCry attack on the NHS in which there was an absence of leadership and a lack of training at the senior level. It was noted that the evolution of NHS Digital and Chief Information Officers over the past few years has improved access to resources during cyber incidents.

With regard to the devices in the scenario, the participants discussed the challenges around the management of smart pumps when they were unfamiliar with the technology. In particular, the team highlighted clinical concerns regarding what would happen if you disconnected a pump and **whether they had safe default modes**. Simple solutions were discussed, such as returning to rudimentary clinical techniques, such as using IV dripping and basing drug dosing on drops and millilitres. A challenge here would be upskilling staff on these calculations.

The fact that clinicians rotate through multiple hospitals a year also means that it is hard to have any workforce fully up-to-date on one healthcare setting's protocols. The nature of NHS training in which junior doctors regularly rotate and move elsewhere, means that **IT issues with Log-ins and passwords are common**. As a result, it is common in the NHS setting to share Log-in details and leave computers open to ensure access is available during emergencies. The team discussed the **impact of these practices in terms of cyber-hygiene**, noting that while these practices often feel necessary in clinical environments, they may open up vulnerabilities to cybersecurity exploits.

The clinicians focused on patient safety and conferred on the challenges of managing a complex patient list (40 patients) during the incident. They also noted that communication with the public would need to be careful, as they may want to reduce people turning up at the front door but not incur panic. In terms of patient safety, **clinicians shared a sense of uncertainty regarding how to confirm whether devices had returned to normal function**. They were unsure whether responsibility lay with them for ensuring devices were working correctly. In the concluding remarks, there was consensus that in these scenarios the responsibility could not fully rest with the physicians, and the involvement of additional disciplines such as engineers, IT and policy makers, would be necessary for an effective response.

4.2 Scenario 2 (Medical): Managing unwell patients during a cyberattack on the Acute Medical Unit (AMU)

Summary of Scenario

This scenario centred on the participant arriving for their shift in the Acute Medical Unit (AMU) when the ward manager informs them the hospital may have been targeted by a cyberattack. Consequently, access to radiological imaging or blood test results is no longer available. The smart pumps available on site could have also been compromised. In addition, the Arterial Blood Gas (ABG) machine that could otherwise be used as an alternative is also apparently malfunctioning, producing some identical results for multiple patients. The participant is asked how they would prioritise four patients with different serious conditions admitted from the Emergency Department, followed by addressing the other 24 patients in the ward. The participant is then asked how they would be able to determine which devices are safe to use, who would they contact to raise concerns about the devices, and how this may impact their decision-making.

Discussion of Scenario

The group quickly recognised and agreed that there are **established hospital procedures** in this case and that they would prioritise patients using the Airways-Breathing-Circulation-Disability-Exposure (ABCDE) method. They went on to agree that they could cover the basic diagnostics with non-technological techniques and set out the order of priority based off this method. They did, however, raise concerns over the ABG machine showing the same results which would make diagnosis difficult. As such, they agreed that raising a **Major Incident** within the hospital at this point would be a good idea. They believed that each of the four patients could start some form of treatment, which would ultimately be targeted at reducing risk of misdiagnosis.

Participants then reflected on their own experiences in hospital settings, including the response during the 2017 WannaCry cyberattack and their need to return to paper notes and simple blood tests. Other participants were interested in how long it took for the situation to return to normal, which, in their case, was two days but they did note it would depend on the hospital. A participant raised an interesting organisational culture point that, within the NHS, **staff may assume that an issue is being escalated by someone else**.

Regarding the question of how to assess whether medical devices were working as expected, one participant highlighted that there were contingency plans in place for this eventuality, with others discussing that there are **onsite medical physics or engineering staff** who can be relied upon to assess the equipment. Alternatives discussed included reverting to using more rudimentary devices, although there were concerns whether they were still in warranty. There were some divergent opinions over **the availability of back-up patient notes in different hospitals**. Regarding escalating the issue, there was consensus that they would escalate it to the hospital's site manager, given their role looking after the entire hospital.

On the question of bringing back devices after a cyberattack, participants mentioned that each device would be **tested, using safe-mode to provide diagnostics information and ensure it is behaving as expected and calibration measures to ensure measurements are accurate**, with the latter being suggested as a potential for use to identify if devices have been impacted by a cyberattack. It was highlighted that some tests automatically publish to computer systems whilst others produce a printout, and these are managed by point-of-care teams. Some group members indicated great confidence in these teams and believed they would not allow devices to go back online unless they were certain they were safe. A point that was stressed was **the need for greater communication between teams**, although one participant noted that this communication had improved over the last five to ten years.

Finally, the group reflected that the scenario had made them **worry about the trust they place on medical devices they use on a regular basis**. One participant raised that the ability to challenge a medical device would depend on a clinician's experience. In an animated discussion, participants discussed that they were **unlikely to challenge results from medical devices unless significantly abnormal diagnostics were produced**. TThere was agreement that it was everyone's responsibility to be careful and follow procedures in the event of a cyberattack. The conversation concluded that, whilst there are contingency plans for cyberattacks causing system outages, the procedures are less known or clear if only some devices become compromised, potentially by malicious actors.

4.3 Scenario 3 (Medical): Treating blind – Patient care during a radiological cyberattack

Summary of Scenario

In this scenario, a healthcare professional within the Acute Medical Unit (AMU) of an incredibly busy hospital is presented with a situation where the hospital is currently experiencing a system-wide cyberattack that has compromised several NHS sites simultaneously. The hospital site manager informs the team that the Electronic Health Records (EHR) system is unavailable and the IT team on site recommends against the use of the radiological imaging system (PACS) upon which clinicians would normally rely to treat the patients with critical conditions present in the AMU at that time. At the time, it is unclear if the PACS system failures are being caused by the cyberattack, a malfunction in the algorithms, or a combination of these factors. While dealing with the uncertainty caused by these critical technical failures, the participant must urgently attend to the critical patients without radiological investigation results available.

Discussion of Scenario

The discussion started with an exploration of the challenges associated with patient care during a cyberattack compromising radiological imaging technology in a hospital setting. A participant noted that Magnetic Resonance Imaging (MRI) devices can be a major source of liability for NHS hospitals. Examples were provided, for instance, if MRI devices cause interference with pacemakers or other electronic devices, which may cause harm or even death to patients.

Addressing the question of how to prioritize patient care, all participants agreed that **the cyberattack and technological failure significantly affected the quality of care**. One of the critical patients would need urgent prioritisation and would very likely need neurosurgical intervention. Other critical patients may need to be transported to another facility for imaging, in order to make an accurate diagnosis and receive treatment. However, some participants highlighted that transferring patients to another hospital might not be a suitable option as the cyberattack compromised several NHS sites simultaneously.

Next, the group discussed how to determine whether the systems and devices being utilized (e.g. radiological imaging devices) are functioning properly. A participant noted that any assessment of medical systems and devices in a hospital setting must follow a team approach. It was explained that in the event of a cybersecurity breach, clinicians must consult with hospital administrators and the IT specialists on site. As a result, they must remain vigilant and report any technical issues carefully, in case hackers mask compromised devices to make them appear temporarily safe and functioning accordingly. Another participant noted that a **business continuity model is required in healthcare settings in the event of a malfunction of systems or devices**. This should allow IT personnel to have more time to focus on managing the system, while clinicians will be able to focus on patients.

Some participants expressed concerns about the safety and performance of these devices, and when and to whom they would communicate these concerns. They highlighted that the NHS operates in a hierarchical manner, so the first steps should always be communicating to ward and hospital site managers and the IT personnel. Further communication with other local and regional NHS sites potentially affected by the security breach was also deemed necessary. A participant highlighted that, in case of a cybersecurity breach affecting critical systems, the patients should also be informed, though one needs to consider the communications carefully to minimise the risk of panic among the public. It was also deemed imperative to document everything carefully in writing. Another participant suggested **reporting any system or device failures to the Medicines and Healthcare products Regulatory Agency (MHRA)** (UK regulator for medicines, medical devices, and blood components for transfusion) in order to initiate an investigation. **Contacting the device manufacturer** of the PACS equipment was also highlighted as important. It was also recommended that clinicians should wait for the official NHS announcement to confirm that the systems or devices are operational again and functioning accordingly.

There was extensive discussion about the reliability of digital healthcare systems and medical devices in the group. Participants expressed scepticism around using IT in the NHS, pointing out that **a considerable number of NHS digital systems are outdated, are not updated regularly, and have been in use for over 10 years**. There was further discussion regarding the challenges clinicians face when dealing with compromised digital records, devices, machinery, or systems, especially if a cyberattack occurred, as it is often hard to identify the root cause or entry point that made the compromise possible. Questions were also raised about the clinicians' training about new software, medical devices, or systems that have an artificial intelligence component or are based on machine learning. It was highlighted that there is insufficient training around new digital technologies and that hospitals generally deal with new device training in isolation.

4.4 Scenario 4 (Surgical): Mother, baby and spinal cord stimulator

Summary of Scenario

The scenario involved a clinician in the Obstetrics ward given the task of preparing the management plan for a pregnant patient (38 weeks) with a closed-loop spinal cord stimulator, who arrives at a busy district hospital at the weekend, presenting signs of labour. The clinician is simultaneously informed that the hospital may be experiencing a system-wide cyberattack, making radiological imaging and laboratory tests temporarily unavailable. The patient informs the clinician that, at her last antenatal appointment, she was told that her baby is in breech position. The patient had no preanesthetic evaluation and there was no advance communication about her spinal cord stimulator. Radiological imaging of the spinal cord stimulator cannot be performed as the systems are down due to the cyberattack. Electronic health records are also unavailable. The group was presented with material explaining the difference between an open-loop and a closed-loop spinal cord stimulator. Parameter changes in an open-loop implantable can be performed only by the clinician, patient, and manufacturer; closed-loop spinal cord stimulators automatically adjust their response (electrical pulses) based on sensor inputs from changes in posture.

Discussion of Scenario

The group quickly agreed that, since the patient had presented to hospital in labour and given the breech position of the baby, the urgent medical response is to perform a Caesarean section (C-section) under general anaesthetic, rather than local epidural in the spine. This would avoid direct intervention around the site where the spinal cord stimulator is located, especially as radiological systems are down due to the cyberattack, so it is not possible to know the exact location of the implantable. The group then discussed the clinical implications of dealing with a closed-loop neuromodulation system for patients needing this kind of urgent care. It was noted that **a lot of patients with implantables arrive at hospital without the device card or the manufacturer's brochure**, so it is hard for clinicians to know the exact model, serial number, or device type. If the patient is conscious, then staff can talk to them and the medical engineers on site to learn more about the device, but in most cases, patients who arrive at accident and emergency departments need urgent medical care or intervention and may not be fully conscious.

Several participants emphasised that, in the case of the pregnant patient in the scenario, **it is not possible to establish whether the device is functional and performing as intended**, given the urgent nature of the patient's condition (and without conducting further tests). For instance, if the patient is experiencing back pain, it would be hard to establish whether it is caused by the patient being in active labour or by the device having potentially interacted with the body in such a way that it has triggered labour. A neurologist could be called to go through the case, but the scenario takes place at night, when specialists are not on call. **Participants also highlighted that it is not possible to know how the patient's body has been communicating with the device, and the device's response**, given that the patient had gone in labour. As it is a closed-loop implantable, the device may have over or under-responded to the effect of the contractions on the patient's body posture (i.e. over or under stimulating the spine). It was also noted that the device could slip out of place as a result of severe contractions. Furthermore, it was noted that the device could interfere with the surgical equipment during the C-section, raising the risk for both mum and baby. Lastly, it was noted that the risk in this scenario is not medical per se (i.e. a C-section for a pregnant patient with a baby in breech position). The **risk comes from the unfamiliarity of the situation, especially if not much is known about the behaviour of the device, whether it is functioning as intended, whether it can be switched on and off**, and the unknown effect it may have on the patient. It was also noted that, currently, clinicians and healthcare professionals come across implanted devices relatively infrequently (i.e. in the small hundreds) and that, ideally, a specialist (a neurologist) should be on call.

The discussion then focused on **whether this case would be flagged as one in which the device may have had an adverse outcome or whether it would be picked up in audit**. Some participants responded that it is unlikely to be flagged if the patient responds well to the surgery, and both mum and baby are safe. The assumption is that the device is not malfunctioning and the clinician focuses on the medical emergency, treating what they see. Another participant noted that, if the healthcare professional suspects something is not right, they would go through **the "five whys" technique** (i.e. starting with an initial description of the problem and then asking "why" until there is a response that can be acted on) to get more information about the root cause of a potentially adverse outcome. If something did go wrong and the device performance is suspected, **one would need to look at the device records and logs**. TThat said, participants acknowledged the limitations associated with investigating devices after an adverse outcome had occurred and that it is sometimes hard to derive conclusive evidence from device logs alone. Equally, it is hard to tell whether it was a hardware (e.g. battery, the sensors) or a software problem, when the malfunction might have occurred, and how it interacted with the body, and vice-versa. Lastly, **several participants agreed that the link between a potentially adverse outcome and the closed-loop implantable would be hard to establish**. This could put the decisions of clinical and healthcare staff in question, raising concerns about professional responsibility and even liability. Several group members highlighted the **considerable information asymmetry between device manufacturers and clinicians when it comes to medical devices** in general. This is more acute for new connected or intelligent implantables such as the one in the scenario. It was discussed that the incentives that manufacturers and healthcare staff have are different, and this is one of the reasons why this discrepancy appears. Participants reflected on the need to have new ways of co-opting manufacturers to provide information about their devices in a more transparent and easier to digest form to healthcare professionals, in addition to the technical information provided to medical engineers inventorying these devices in hospital.

4.5 Scenario 5 (Emergency): Patient care and autonomous ventilators

Summary of Scenario

The scenario involved a member of staff in the Intensive Care Unit (ICU) being debriefed at the start of their shift about a patient on a ventilator, whose oxygen saturation levels suddenly dropped, requiring manual resuscitation. The ventilator operated in one setting when actually displaying another, potentially due to a problem with the ventilator's software or firmware. The cause of the event is initially attributed to either a mode change by the nurse or a device malfunction given recent reports about similar ventilators being hacked. During the debrief, other ICU patients start developing respiratory distress with oxygen desaturating rapidly. The scenario raised questions about vulnerable systems in emergency and intensive care, the risks of closed-loop life support systems, and the measures to be taken to ensure safe use of AI-based, automated systems in critical medical settings.

Discussion of Scenario

The discussion first explored the **seriousness of relying on vulnerable or malfunctioning devices and systems in emergency and intensive care units**, as well as the risks associated with the use of AI-based, automated medical devices. The group acknowledged that these systems can be prone to new kinds of malfunctions and vulnerabilities, with direct consequences for patient care. Participants cited a recent incident, where IT servers broke down at a hospital due to a heatwave, resulting in the cancellation of operations, as an example of the system's reduced resilience and its reliance on digital technologies. It was noted that the reliance on paper notes could have led to chaos if a cyberattack had occurred. However, participants disagreed about the exposure of the healthcare system to these kinds of vulnerabilities and also about the extent to which AI-based medical devices are currently used in hospitals. However, the group concluded that every medical device or system that automatically adjusts can be vulnerable to sometimes undetectable malfunctions.

Considering this, the group explored **the risks of closed-loop life support systems and medical systems based on Artificial Intelligence (AI) in acute medical settings**. While some participants noted that closed-loop automated systems are predominantly used in ventilation, many emphasized that relying entirely on an automatic system would cause severe issues if the system failed, highlighting a general issue of trust. In addition, most participants specified that they did not know how many of the machines worked, making it even more challenging to assess their performance.

Participants then discussed the hypothetical instance where one of the patients in the scenario had died, considering **the appropriate post-mortem investigations that would need to be conducted**. The group disagreed about the likelihood of these malfunctions happening at the moment. They also raised the possibility of intentional system alteration but acknowledged the existence of a log to track any changes. Ultimately, they agreed that while medical devices experience malfunctions, human controls are and should be in place. The group expressed curiosity in exploring the process of determining the cause of death and the assignment of responsibility for it.

The group engaged in a comprehensive discussion regarding **measures and protocols aimed at ensuring the safety and appropriate functioning of connected and intelligent medical devices**. While acknowledging the importance of risk assessments conducted by clinical safety officers, they expressed concerns regarding information distribution and the unavailability of safety officers during vulnerable periods. Human error and hacking were also deliberated, with a specific emphasis placed on the significance of immediate and internal reporting in cases where suspicions of potential problems arise. The conversation also addressed the complex issue of understanding the performance and outputs from AI-based medical devices, especially those based on continuous learning, and the reduced transparency associated with their functionality. The group underscored the importance of reporting any concerns, which ties into previous discussions regarding shared liability and communication among hospital staff. Participants explored possible strategies for creating a comprehensive infrastructure for monitoring and ensuring the safety of connected and intelligent medical devices to address these challenges. The group highlighted that the adoption of technologies with the potential to cause harm should be carefully considered.

Participants also discussed concerns regarding **the reliability of AI-based or automated medical devices**, including the potential for malfunction and adverse patient outcomes. Responsibility for harm caused by such malfunctions was debated, with participants offering varying opinions on who should be held accountable. There was no clear agreement on how responsibility should be apportioned, though some argued that manufacturers should have more responsibility for ensuring that their devices were developed to high standards and checked and maintained regularly. Other participants questioned whether clinicians could be held accountable for malfunctions they had no control over, such as those from AI-based, automated devices. Careful and rigorous device risk management processes were recommended for all hospital settings. Clear protocols and procedures were also deemed necessary to ensure safe and reliable use of such devices.

4.6 Scenario 6 (community): Seizure outbreaks in epilepsy management apps

Summary of Scenario

The scenario covered a 17-year-old girl presenting herself at the General Practitioner (GP) with a relapse in epileptic seizures while scrolling through an epilepsy management app on her phone. The patient had been diagnosed with epilepsy 10 years ago, which had been well-controlled with medication, and she had been free of seizures for the past three years. Prior to the new seizures, she reported feeling well, taking her medications regularly, and not experiencing other symptoms. She was a regular on the support forum on her epilepsy management app. The GP suspects that the patient's use of the app may have triggered the seizures and that the app's forum may have been the target of cybercriminal activity. There have previously been virtual assaults on epilepsy patients by hackers who change the screen brightness of those using social media sites to trigger epileptic seizures. Scenario participants are tasked with coming up with a management plan for the patient while considering the wider population health implications of this case.

Discussion of Scenario

The discussion started with analysing how cyberattacks that change the screen brightness affect patients who suffer from photosensitive conditions such as epilepsy and migraines. Participants noted that **these attacks could cause symptoms such as seizures, headaches, distress, loss of vision, loss of focus, visual effects, compromise to the airway, choking if they were eating at the time, and in some cases, insomnia**. Participants also suggested that other at-risk patient groups from similar attacks could be **dementia patients, or those with neurodiverse conditions; while chronic exposure may impact people with insomnia and certain retinal diseases**. There was also discussion on how such an attack could be carried out. Participants theorized that hackers could reverse-engineer open-source software to change the script behind the app to cause changes to the screen brightness, and in some cases even cause the battery to explode. Participants wondered what the role of the physician is in this scenario, given that the relationship is largely between the providers of the application and the user, unless the app was prescribed. Any points of liability would need further investigation and could not be easily determined.

Participants then considered where these concerns could be reported to and/ or communicated. There was consensus that **such cases should ideally be taken to the police as it involved a hacker attempting to cause actual harm to a victim**. It was further suggested that **public health authorities, NHS England (Cyber Department)** or the Ministry of Defence could also be considered for reporting. It was also raised that, if malicious intent is not established in the first instance, it may make sense **to also contact the application provider and the app store**, to make them aware of both the flickering screen brightness, and the adverse effects it has on users and vulnerable groups. Discussion turned to whether there were any measures or protocols in place by physicians, GP practices, or hospitals to ensure concerns on using these medical apps are communicated to the appropriate authorities. Participants unfortunately concluded that **there are no agreed safeguards**, and that in the face of such incidents, physicians would likely advise that patients stop using the app, which may be detrimental for patients who are dependent on this support.

Participants acknowledged that patients frequently use digital platforms to find support groups and information, however conceded that **such use throws up challenges for healthcare professionals as they cannot control or predict the harmful effects that hacks may have on patients**. Participants also discussed that, currently, there are no epilepsy support apps that NHS doctors specifically endorse, although some may be recommended via word-of-mouth and patient recommendations. While healthcare professionals are aware of the existence of these apps, there are multiple on the market, and they are unable to keep track of them all or recommend any particular apps.

The challenges faced physicians in the aftermath of a cyber-attack were also discussed. Participants felt that there was a **general lack of awareness among clinicians on signs of a cyberattack, and contingency methods if such an attack takes place**. They stressed the **importance of carrying out knowledge sessions on how to treat patients if electronic systems are unavailable as well as who to contact to get systems back online**. Participants also touched upon the reputational risk to the NHS if patients discover that their systems are vulnerable to cyber-attacks. The discussion also covered the fact that cloud-based services were perceived more susceptible to cyberattacks, as on-site services have fewer points of vulnerability.

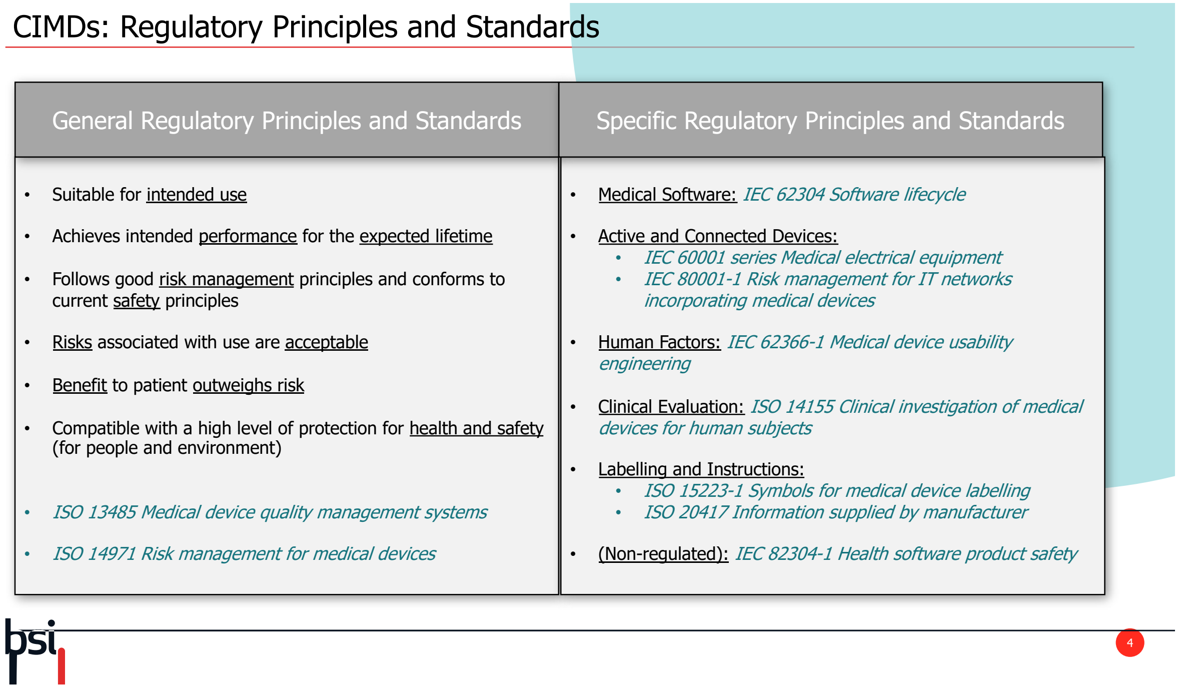
5. The Role of Standards, Regulations, and the Changing Policy Landscape

The event concluded with presentations and a panel discussion led by Reg-MedTech project partners at the BSI – the UK's National Standards Body. The session addressed the latest developments in standards, guidance, and regulations pertaining to connected and intelligent medical devices. The panel was composed of the following members:

- **Rob Turpin**, Head of Healthcare Sector, BSI
- **Tim McGarr**, Head of Digital Sector, BSI
- **Paul Sim**, Medical Devices Knowledge Manager, BSI
- **Emma Glass**, Universities Partnership Manager, BSI

Rob Turpin opened the session with a talk highlighting the close relationship between voluntary standards and mandatory regulations in the medical device field. Regulations are devised to ensure the safety, performance, and security of medical devices placed on the market, including software. In the UK, the MHRA (the regulator) appoints Approved Bodies (such as BSI) to undertake conformity assessment. It was noted that the UK has diverged from EU Medical Device Regulations since Brexit and is now producing its own legislation, which is expected to the brought into force by July 2024. The presentation also highlighted that medical devices are classified in accordance with their "intended use" and their risk profile. For instance, a patient monitor is classed as a medium risk device, while a pacemaker would be classed as high risk. In this context, standards can be written as requirements in line with medical device regulations, test methods, codes of practice, or guidance. Several standards that address both general and specific regulatory principles were noted, as seen below in this presentation snapshot (Figure 3).

The role of harmonized standards, which allow manufacturers to demonstrate presumption of conformity to EU Medical Device Regulations was also discussed, and the example of *EN ISO 14971: 2019 Medical Device Risk Management* was provided, showing how it maps to regulatory requirements.



CIMDs: Regulatory Principles and Standards

General Regulatory Principles and Standards	Specific Regulatory Principles and Standards
• Suitable for intended use • Achieves intended performance for the expected lifetime • Follows good risk management principles and conforms to current safety principles • Risks associated with use are acceptable • Benefit to patient outweighs risk • Compatible with a high level of protection for health and safety (for people and environment) • *ISO 13485 Medical device quality management systems* • *ISO 14971 Risk management for medical devices*	• Medical Software: *IEC 62304 Software lifecycle* • Active and Connected Devices: • *IEC 60001 series Medical electrical equipment* • *IEC 80001-1 Risk management for IT networks incorporating medical devices* • Human Factors: *IEC 62366-1 Medical device usability engineering* • Clinical Evaluation: *ISO 14155 Clinical investigation of medical devices for human subjects* • Labelling and Instructions: • *ISO 15223-1 Symbols for medical device labelling* • *ISO 20417 Information supplied by manufacturer* • (Non-regulated): *IEC 82304-1 Health software product safety*

4

Figure 3: Example of scenario worksheet used during the event

Turpin also noted that, in the UK, the MHRA set up the *"Software and AI as a Medical Device" Change Programme*, intended to address some of the new data quality, cybersecurity, and algorithmic trustworthiness challenges raised by software-based medical devices and software as a medical device (SaMDs), including AIaMDs. The MHRA has been working with BSI and other institutional partners such as the NHS and the National Institute for Health and Care Excellence (NICE) to ensure that emerging regulations, guidance, and standards address most of these challenges. Several BSI-led initiatives linked to the programme were presented, including the current review of software lifecycle best practices for medical devices (IEC 62304), several standards initiatives to support human-centred medical software and AI, and standards mapping for Good Machine Learning Practices (GMLP).

Tim McGarr followed with a presentation addressing the latest developments in cybersecurity and artificial intelligence standards more generally. It is expected that several of these standards will need to be applied or mirrored in the healthcare sector more broadly, including for the development, management, and monitoring of connected and intelligent medical devices. These standards could also inform updates to existing medical device standards, so that they better address critical digital technology issues. McGarr noted that the *ISO/IEC 27000 series of standards comprehensively addresses cybersecurity aspects and best practices, including the ISO/IEC 27001: Information Security Management Systems* framework standard, which is widely used by organisations around the world.

Special attention was given to the ISO/IEC 42001: AI Management System standard, which is currently in development and due to be published in 2023. The standard specifies the requirements and provides guidance for establishing, implementing, maintaining, and continually improving an AI management system within the context of an organisation. The standard is thought to help organisations develop and manage AI systems responsibly and to meet some of emerging regulatory requirements for AI. The presentation also highlighted the work currently undertaken in the UK's Artificial Intelligence Standards Hub, a government-backed initiative between the Alan Turing Institute, BSI, and the National Physics Laboratory (NPL). The Hub's mission is to advance the responsible development and use of AI in the UK, to help stakeholders navigate the international AI standards landscape, and to participate in the development of new standards based on critical stakeholder needs.

The panel discussion that followed highlighted the importance of having the voice of critical stakeholders such as clinicians, healthcare professionals, and researchers captured in the development of standards in this field. **Emma Glass** pointed out the importance of training and educating these stakeholders about the role and value of standards, especially given the need to follow best practices when developing but also when monitoring the performance of medical devices deployed and used in hospital settings. Glass highlighted that the BSI is currently delivering several workshops across higher education institutions on the nature, role, and value of standards in different areas, including healthcare. Several discussions during the event, including in this panel, pointed at the value of more training for clinicians and healthcare professionals about the identification and management of potential device malfunctions caused by AI or cyberattacks.

Paul Sim highlighted the critical importance of having clinicians' input in the development of medical device standards, especially in standards such as *IEC 60601-Part 2 series*, which address the basic safety and essential performance of different types of medical devices, from ventilators and anaesthetic systems to X-ray machines and MRIs (and many more). Sim noted that, from his engagement with medical professional bodies, it is difficult for clinicians to get time release for engagement in standards development. However, clinicians' input is critically important to ensure the latest understanding of device use patterns, vulnerabilities, malfunctions, and failures at the point of care is captured in standards updates and new standards development.

Sim also highlighted that a more coordinated approach is needed when tackling the challenges associated with emerging digital technologies embedded in or fully classed as medical devices. He provided the example of how teamwork in the aviation industry, especially in a cockpit setting, could be replicated in the healthcare sector and why, currently, we don't see the same level of synergetic communication and learning between critical stakeholders such as manufacturers, clinicians, and healthcare professionals.

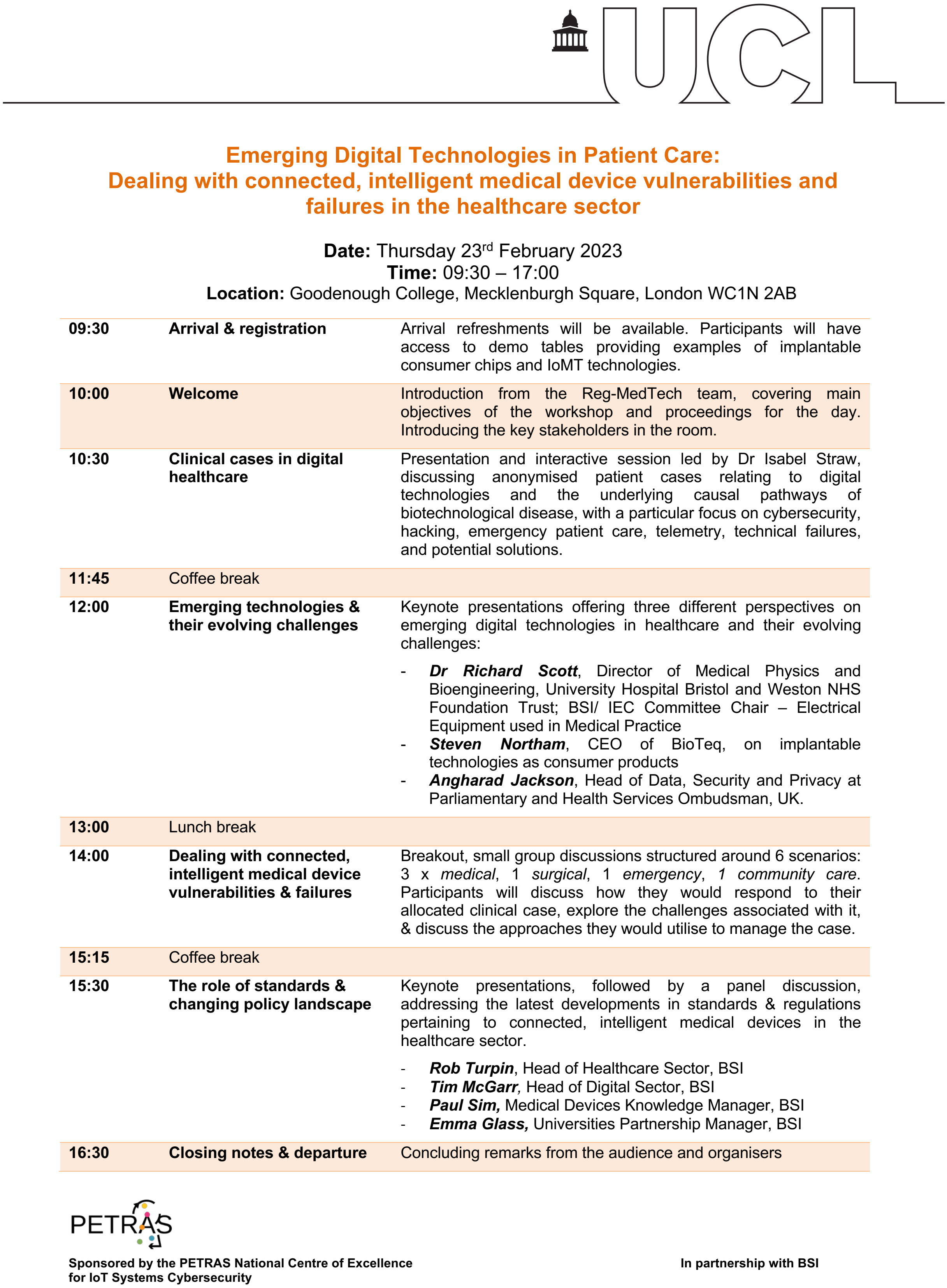
Sim also pointed at several critical issues discussed throughout the event. First, the growing importance of including the patient's voice in communications about medical devices that, up to now, might have predominantly been between clinicians/ healthcare professionals, manufacturers/ developers, and regulators. Second, he noted the discrepancy between medical device design and the expectations that healthcare professionals in a hospital setting might have from that device, referencing oxygen supply systems during the Covid-19 crisis in the UK. He made the audience aware of the Healthcare Safety Investigation Branch

(HSIB), set up by the UK government to improve patient safety through independent investigations of systems and processes in healthcare. BSI have worked closely with the HSIB when needed. Lastly, Sim stressed the importance of thinking about the device use from the early development stages and about the importance of rethinking the monitoring of devices at the postmarketing phase (once they are deployed and in use).

6. Concluding Remarks

The event concluded with a short address from the organisers about the importance of tackling issues arising from connected and intelligent medical devices through a multi-professional and multidisciplinary lens. It was recognised that more needs to be done to ensure that best practice for device development and healthcare management are rooted in an understanding of the challenges faced by professionals at the frontline, together with patient and user expectations, and more appreciation of the new players (e.g., cloud providers) who are becoming more and more relevant in this space.

Annex 1: Workshop Agenda



UCL

Emerging Digital Technologies in Patient Care: Dealing with connected, intelligent medical device vulnerabilities and failures in the healthcare sector

Date: Thursday 23rd February 2023
Time: 09:30 – 17:00
Location: Goodenough College, Mecklenburgh Square, London WC1N 2AB

09:30	**Arrival & registration**	Arrival refreshments will be available. Participants will have access to demo tables providing examples of implantable consumer chips and IoMT technologies.
10:00	**Welcome**	Introduction from the Reg-MedTech team, covering main objectives of the workshop and proceedings for the day. Introducing the key stakeholders in the room.
10:30	**Clinical cases in digital healthcare**	Presentation and interactive session led by Dr Isabel Straw, discussing anonymised patient cases relating to digital technologies and the underlying causal pathways of biotechnological disease, with a particular focus on cybersecurity, hacking, emergency patient care, telemetry, technical failures, and potential solutions.
11:45	Coffee break	
12:00	**Emerging technologies & their evolving challenges**	Keynote presentations offering three different perspectives on emerging digital technologies in healthcare and their evolving challenges: - ***Dr Richard Scott***, Director of Medical Physics and Bioengineering, University Hospital Bristol and Weston NHS Foundation Trust; BSI/ IEC Committee Chair – Electrical Equipment used in Medical Practice - ***Steven Northam***, CEO of BioTeq, on implantable technologies as consumer products - ***Angharad Jackson***, Head of Data, Security and Privacy at Parliamentary and Health Services Ombudsman, UK.
13:00	Lunch break	
14:00	**Dealing with connected, intelligent medical device vulnerabilities & failures**	Breakout, small group discussions structured around 6 scenarios: 3 x *medical*, 1 *surgical*, 1 *emergency*, *1 community care*. Participants will discuss how they would respond to their allocated clinical case, explore the challenges associated with it, & discuss the approaches they would utilise to manage the case.
15:15	Coffee break	
15:30	**The role of standards & changing policy landscape**	Keynote presentations, followed by a panel discussion, addressing the latest developments in standards & regulations pertaining to connected, intelligent medical devices in the healthcare sector. - ***Rob Turpin***, Head of Healthcare Sector, BSI - ***Tim McGarr,*** Head of Digital Sector, BSI - ***Paul Sim,*** Medical Devices Knowledge Manager, BSI - ***Emma Glass,*** Universities Partnership Manager, BSI
16:30	**Closing notes & departure**	Concluding remarks from the audience and organisers

PETRAS

Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

In partnership with BSI

Annex 2: Scenarios

Scenario 1: Caring for medical patients during a weekend cyberattack

Scenario
(Patients are referenced by age and sex, e.g., 17M = 17 year-old male)

It's Saturday morning and you are a member of the general medical team. As part of the weekend team, you will be covering a range of medical specialties who are not on site during on call hours, including oncology and neurology. At the morning meeting you are informed by the hospital site manager that there has been a cyberattack overnight which has compromised the wireless network of the hospital, the computing systems, and some of the supporting online platforms. Now that the computing systems are down, you cannot access radiological or laboratory reports and do not have blood results for the patients. The hospital site manager also shares concerns regarding the current use of smart pumps on the wards, which have recently been demonstrated to have several cybersecurity vulnerabilities [1-5].

0930 – During the medical handover you are told about the following patients who require attention:

1. **Mr Chemo & Mrs Infusion:** Two patients on the oncology ward are due to have their chemotherapy over the weekend, however the online chemo-prescribing platform has been compromised and you do not have access to their previous records or lab results [6].
2. **Mr Pancreas:** Mr Pancreas was admitted overnight with severe vomiting, dehydration, and confusion, related to end-stage metastatic pancreatic cancer. He was started on the palliative care pathway, however the syringe drivers for palliative medication have not yet been prescribed.
3. **Mrs Sugar:** Mr Sugar is a 21M with type 1 diabetes who was admitted with Diabetic Ketoacidosis (DKA) and started on an insulin infusion. She requires review due to increased confusion and vomiting.

Aside from the four patients handed over to you, there are 42 medical patients across the different wards that you are responsible for, who have a range of common medical problems including acute illness in the elderly, asthma exacerbations, chest infections, ischaemic heart disease, kidney injury and alcohol withdrawal.

Case-specific questions

1. How will you prioritise the care of these patients and how may this be influenced by the specific risks of the cyberattack?

2. How would you assess whether the systems and devices (e.g. smart pumps) you are using are safe and are behaving/ performing accordingly? Consider that a consequence of this cyberattack is that it is unclear which supporting platforms, devices, and systems have been compromised and which

are working as expected.

3. If you are concerned about the safety and performance of these devices, when, and to whom, do you communicate these concerns?

4. Once IT indicates the systems are no longer vulnerable, what measures are taken (by you or the hospital) to ensure the devices you are using are safe and performing accordingly?

5. What concerns do you have about the reliability of the digital healthcare systems and devices you use or come in contact with? How do these concerns impact your clinical decision-making and professional responsibility?

General questions

1. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?

2. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

3. What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

References

[1] Pycroft, Laurie, and Tipu Z. Aziz. 'Security of Implantable Medical Devices with Wireless Connections: The Dangers of Cyber-Attacks'. Expert Review of Medical Devices, vol. 15, no. 6, June 2018, pp. 403–06.

[2] Adashi, Eli Y., and Nicole M. Thomasian. 'Medical Devices in Harm's Way: Medjacking'. JAMA Health Forum, vol. 1, no. 1, Jan. 2020

[3] 'Symbiq Infusion System: FDA Cybersecurity Warning'. Reactions Weekly, vol. 1564, no. 1, Aug. 2015, pp. 7–7. Springer Link, https://doi.org/10.1007/s40278-015-4150-5.

[4] 'Smart Pumps in Practice: Survey Results Reveal Widespread Use, but Optimization Is Challenging'. Institute For Safe Medication Practices, 4 Apr. 2018,

[5] 'New Report Highlights Challenges of Implementing "Smart" Pump Devices across NHS'. HSIB, 19 Mar. 2021, https://www.hsib.org.uk/news-and-events/new-report-highlights-challenges-of-implementing-smart-pump-devices-across-nhs/.

[6] Ades, Steven, et al. 'Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect'. JCO Oncology Practice, vol. 18, no. 1, Jan. 2022

[7] Faulds, Eileen R., et al. 'Insulin Pump Malfunction During Hospitalization: Two Case Reports'. Diabetes Technology & Therapeutics, vol. 18, no. 6, June 2016, pp. 399–403. PubMed, https://doi.org/10.1089/dia.2015.0434.

[8] Warner, Lindsay, et al. 'Malfunctioning Sufentanil Intrathecal Pain Pump: A Case Report'. Journal of Medical Case Reports, vol. 14, no. 1, Jan. 2020, p. 1. PubMed, https://doi.org/10.1186/s13256-019-2314-2.

[9] Haase, Krystal K., et al. 'Clinicians' Experiences and Reflections from A Health System Cyberattack'. Jaccp: Journal Of The American College Of Clinical Pharmacy, vol. 4, no. 6, June 2021.

[10] Fields, Aaron M., et al. 'Closed-Loop Systems for Drug Delivery'. Current Opinion in Anaesthesiology, vol. 21, no. 4, Aug. 2008, pp. 446–51. PubMed, https://doi.org/10.1097/ACO.0b013e3283007ecc.

Scenario 2: Managing unwell patients during a cyberattack on the Acute Medical Unit (AMU)

Scenario description
(Patients are referenced by age and sex, e.g., 17M = 17 year-old male)

0800am: You are a member of staff on the Acute Medical Unit (AMU) providing care for 28 patients with a range of medical conditions. Overnight the following patients were admitted from the Emergency Department:

- **Mr Sugar:** 85M with Hyperosmolar hyperglycemic state (HHS) on a background of type 2 diabetes, started on IV fluids and insulin due to significant ketonaemia [1-2].
- **Mr Lungs:** 62M with respiratory distress and confusion, diagnosed with an exacerbation of his underlying Chronic Obstructive Pulmonary Disease (COPD).
- **Mrs Heart:** 52F with shortness of breath, cough and fever, on a background of Stage 2 Heart Failure.
- **Mr Kidney:** 68M with Chronic Kidney Disease (CKD) admitted with shortness of breath, peripheral oedema and severe confusion.

On attempting to view the patient notes, you find that Cerner (the Electronic Patient Health Records System) will not open, and the ward manager informs you the hospital may be experiencing a cyberattack. As a result, you no longer have access to radiological imaging or blood test results. The ward manager also shares her concerns regarding the treatments being delivered to the ward patients via smart pumps (including IV medications, fluids, blood transfusions, and insulin) given the recent reports regarding malfunctions and cybersecurity vulnerabilities relating to these pumps [3-9].

Due to the laboratory results being unavailable, the healthcare assistant has been using the ward Arterial Blood Gas (ABG) machine to obtain rudimentary blood tests for each of your patients. Before attending to patients, your team review these results and you quickly notice these seem grossly abnormal with all patients being reported to have severe metabolic acidosis that is not in keeping with their clinical picture [8].

You must now begin your ward round of the 28 patients on the AMU, including reviewing the new patients admitted overnight.

Case-specific questions

PETRAS
Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

1. How will you prioritise the care of these patients and how may this be influenced by the specific risks of the cyberattack?

2. How would you assess whether the systems and devices (e.g. smart pumps) you are using are safe and are behaving/ performing accordingly? Consider that a consequence of this cyberattack is that it is unclear which supporting platforms, devices, and systems have been compromised and which are working as expected.

3. If you are concerned about the safety and performance of these devices, when and to whom do you communicate these concerns?

4. Once IT indicates the systems are no longer vulnerable, what measures are taken (by you or the hospital) to ensure the devices you are using are safe and performing accordingly?

5. What concerns do you have about the reliability of the digital healthcare systems and devices you use or come in contact with? How do these concerns impact your clinical decision-making and professional responsibility?

General questions

1. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?

2. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

3. What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

References

[1] Gosmanov, Aidar R., et al. 'Hyperglycemic Crises: Diabetic Ketoacidosis and Hyperglycemic Hyperosmolar State'. http://www.ncbi.nlm.nih.gov/books/NBK279052/

[2] NICE. Diabetic hyperglycaemic emergencies. Available from: https://bnf.nice.org.uk/treatment-summaries/diabetic-hyperglycaemic-emergencies/

[3] 'Symbiq Infusion System: FDA Cybersecurity Warning'. Reactions Weekly, vol. 1564, no. 1, Aug. 2015, pp. 7–7. Springer Link, https://doi.org/10.1007/s40278-015-4150-5.

[4] 'Smart Pumps in Practice: Survey Results Reveal Widespread Use, but Optimization Is Challenging'. Institute For Safe Medication Practices, 4 Apr. 2018,

[5] 'New Report Highlights Challenges of Implementing "Smart" Pump Devices across NHS'. HSIB, 19 Mar. 2021, https://www.hsib.org.uk/news-and-events/new-report-highlights-challenges-of-implementing-smart-pump-devices-across-nhs/.

[6] Faulds, Eileen R., et al. 'Insulin Pump Malfunction During Hospitalization: Two Case Reports'. Diabetes Technology & Therapeutics, vol. 18, no. 6, June 2016, pp. 399–403. PubMed, https://doi.org/10.1089/dia.2015.0434.

[7] Warner, Lindsay, et al. 'Malfunctioning Sufentanil Intrathecal Pain Pump: A Case Report'. Journal of Medical Case Reports, vol. 14, no. 1, Jan. 2020, p. 1. PubMed, https://doi.org/10.1186/s13256-019-2314-2.

[8] Masayuki, et al. 'Misdiagnosis of High Anion Gap Acidosis Owing to Instrument Error of a Device'. CEN Case Reports, vol. 8, no. 4, Nov. 2019, pp. 308–10. PubMed, https://doi.org/10.1007/s13730-019-00413-4

[9] FDA Report: Smiths Medical Recalls Certain Medfusion 3500 and 4000 Syringe Infusion Pumps for Software Issues That May Impact Infusion Delivery (2022).

Scenario 3: Treating blind – Patient care during a radiological cyberattack

Scenario description
(Patients are referenced by age and sex, e.g., 17M = 17 year-old male)

0830am: You are a member of the medical team on the Acute Medical Unit (AMU) in a busy hospital and have just been informed that the hospital is facing a system-wide cyberattack which has compromised several NHS sites at once [1]. The hospital site manager informs you that the Electronic Health Records (EHR) system is unavailable, and that the IT team have advised against using PACS (the radiological imaging system in your trust) [2-4]. The radiology system is being investigated due to a technological failure that suggests that the images being displayed are inaccurate [5]. At this stage it is not clear whether the PACS system failures are linked to the cyberattack, to algorithmic malfunctions, or a combination of the two.

The following patients have been referred to you from the Emergency Department and for whom you do not currently have any investigation results:

- **Miss Lung:** 24F admitted following a severe asthma attack requiring salbutamol and ipratropium nebulisers and IV magnesium sulphate. Her wheeze has resolved but she is now complaining of increasing left sided chest pain and shortness of breath.
- **Mr Oesophagus:** 84M admitted following a stroke that resulted in left arm and leg weakness with severe dysphagia. He can no longer swallow and requires an NG tube for feeding and his regular medications (antihypertensives and antiepileptics).
- **Mrs Legs:** 61F admitted with 6-hour history of lower back pain, bilateral burning leg pain and urinary incontinence, with a background of degenerative disc disease.
- **Mr Brain:** 30M admitted following with a severe headache, pain when looking at lights, vomiting and drowsiness.

Case-specific questions

1. How will you prioritise the care of these patients and how may this be influenced by the specific risks of the cyberattack and the radiological software not performing accordingly?

2. How would you assess whether the systems and devices (e.g. radiological imaging system) you are using are safe and are behaving/ performing accordingly? Consider that in this case, it is not clear why the PACS system is not performing accordingly.

3. If you are concerned about the safety and performance of these devices, when and to whom do you communicate these concerns?

PETRAS

Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

4. Once IT indicates the systems are no longer vulnerable, what measures are taken (by you or the hospital) to ensure the devices you are using are safe and performing accordingly?

5. What concerns do you have about the reliability of the digital healthcare systems and devices you use or come in contact with? How do these concerns impact your clinical decision-making and professional responsibility?

General questions

1. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?

2. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

3. What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

References

1. Ghafur, S., et al. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS'. Npj Digital Medicine, vol. 2, no. 1, Oct. 2019, pp. 1–7. www.nature.com, https://doi.org/10.1038/s41746-019-0161-6.

2. Anderson T, Torreggiani W.C. 'The Impact of the Cyberattack on Radiology Systems in Ireland'. Ir Med J; Vol 114; No. 5; P347. Available at: https://imj.ie/wp-content/uploads/2021/05/The-Impact-of-the-Cyberattack-on-Radiology-Systems-in-Ireland.pdf

3. Dameff, Christian, et al. 'Cyber Disaster Medicine: A New Frontier for Emergency Medicine'. Annals of Emergency Medicine, vol. 75, no. 5, May 2020, pp. 642–47. ScienceDirect, https://doi.org/10.1016/j.annemergmed.2019.11.011.

4. Eichelberg, Marco, et al. 'Cybersecurity Challenges for PACS and Medical Imaging'. Academic Radiology, vol. 27, no. 8, Aug. 2020, pp. 1126–39. ScienceDirect, https://doi.org/10.1016/j.acra.2020.03.026.

5. FDA (2022). Class 2 Device Recall ZAPX (Treatment Delivery). Available at: https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=195555

Scenario 4: Mother, baby and spinal cord stimulator

(Patients are referenced by age and sex, e.g., 17M = 17 year-old male)

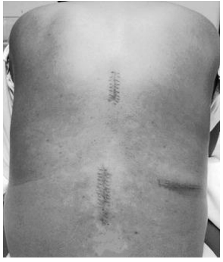
Scenario description

You are covering the Obstetrics ward during a weekend shift at a busy district general hospital (DGH). On arriving to the ward, the nursing team ask you to review a **Ms Spine** - a patient who has just arrived. At the same time the ward manager also informs you that the hospital may be experiencing a system-wide cyberattack, and as a result you do not have access to radiological imaging or laboratory tests [1-4].

Ms Spine is as 29F patient (Gravida 3, Para 2) with an intrauterine pregnancy at 38 weeks and 3 days' gestation who has presented to the labour and delivery unit in active labour. The patient quickly informs you of her past medical history, which includes a motor vehicle accident 2 years ago (occurring after the birth of her last child) that left the patient with lower back pain and bilateral neuralgias [5]. For these symptoms she underwent placement of a closed-loop spinal cord stimulator that auto-adjusts based on her posture. (*Participants can find further details on the spinal cord stimulator below).*

Aside from her back surgery, Ms Spine has a history of well-controlled asthma and her previous pregnancies were uncomplicated with normal vaginal deliveries. Her current pregnancy has progressed without complication, however at the last appointment she was informed that the baby was in breech position. For reasons unknown, Ms Spine has not had a preanesthetic evaluation before she presented herself and there has been no advance communication regarding her SCS [5]. Unfortunately, you do not have access to radiological imaging of the spinal stimulator due to electronic health records being disrupted by the cyberattack. However, on examination you observe the findings presented in Figure 1.

Figure 1: Clinical examination of Ms Spine - Visual inspection revealed 1 horizontal scar and 2 midline vertical scars, corresponding to previous lead implantations for her stimulator.

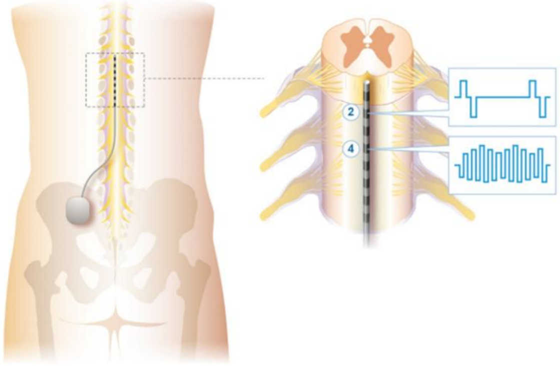


You must come up with a management plan for Ms Spine and consider the implications of her implanted technology for both herself and the baby.

Background on Closed-Loop Spinal Cord Stimulators

Spinal cord simulation (SCS) delivers electrical pulses via epidural electrodes on the dorsal side of the spinal cord to treat pain. The technology was first introduced in the 1980s, at which time it consisted of the implanted pulse generator, electrodes, and wireless handheld controller (Figure 2). Initially the technology was open-loop, such that the patient/clinician was responsible for parameter changes, however in the closed-loop systems that now exist, the stimulator automatically adjusts based on sensor inputs [6]. The most advanced versions of this technology include artificial intelligence (AI)-based SCS system, such as Senza HFX. Changes in posture can result in changing distance between the stimulation leads and the target tissue, causing variability in the simulation. Closed-loop systems were first explored to create posture-responsive stimulation, in which an accelerometer could detect patient movement and adjust stimulation accordingly [6-7]. Other examples of closed-loop (CL) neuromodulation include CL Deep Brain Stimulation for Parkinsons [8].

Figure 2: An implanted spinal cord stimulation system with a lead positioned in the epidural space is used to deliver multiplexed stimulation patterns to differential targets.



Case-specific questions

1. What are the risks of a compromised spinal cord stimulator during pregnancy, and how could a compromised device affect a fetus? In this particular case, what are the clinical implications of dealing with a closed-loop neuromodulation system for patient care?

2. How would you assess whether the medical device (i.e. the closed-loop spinal cord stimulator) is performing accordingly?

3. If you are concerned about the safety and performance of these devices, when and to whom do you communicate these concerns?

4. What measures and protocols are taken (by you or the hospital) to ensure that similar patient devices you may come in contact with are safe and are performing accordingly?

5. Do you have concerns about the reliability of AI-based or automated medical devices? If so, how does this impact your clinical decision-making and professional responsibility?

General questions

1. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?

2. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

3. What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

References

1. Ghafur, S., et al. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS'. Npj Digital Medicine, vol. 2, no. 1, Oct. 2019, pp. 1–7. www.nature.com, https://doi.org/10.1038/s41746-019-0161-6.

2. Anderson T, Torreggiani W.C. 'The Impact of the Cyberattack on Radiology Systems in Ireland'. Ir Med J; Vol 114; No. 5; P347. Available at: https://imj.ie/wp-content/uploads/2021/05/The-Impact-of-the-Cyberattack-on-Radiology-Systems-in-Ireland.pdf

3. Dameff, Christian, et al. 'Cyber Disaster Medicine: A New Frontier for Emergency Medicine'. Annals of Emergency Medicine, vol. 75, no. 5, May 2020, pp. 642–47. ScienceDirect, https://doi.org/10.1016/j.annemergmed.2019.11.011.

4. Eichelberg, Marco, et al. 'Cybersecurity Challenges for PACS and Medical Imaging'. Academic Radiology, vol. 27, no. 8, Aug. 2020, pp. 1126–39. ScienceDirect, https://doi.org/10.1016/j.acra.2020.03.026.

5. Patel, Suhas, et al. 'Urgent Cesarean Section in a Patient with a Spinal Cord Stimulator: Implications for Surgery and Anesthesia'. The Ochsner Journal, vol. 14, no. 1, 2014, pp. 131–34. PubMed Central, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3963044/.

6. Vallejo, Ricardo, et al. 'A New Direction for Closed-Loop Spinal Cord Stimulation: Combining Contemporary Therapy Paradigms with Evoked Compound Action Potential Sensing'. Journal of Pain Research, vol. 14, Dec. 2021, pp. 3909–18. PubMed Central, https://doi.org/10.2147/JPR.S344568.

7. Schultz, David M., et al. 'Sensor-Driven Position-Adaptive Spinal Cord Stimulation for Chronic Pain'. Pain Physician, vol. 15, no. 1, 2012, pp. 1–12.

8. Zanos, Stavros. 'Closed-Loop Neuromodulation in Physiological and Translational Research'. Cold Spring Harbor Perspectives in Medicine, vol. 9, no. 11, Nov. 2019, p. a034314. PubMed Central, https://doi.org/10.1101/cshperspect.a034314.

Scenario 5: Patient care and autonomous ventilators

Scenario description

(Patients are references by age and sex, e.g., 60M = 60-year-old male)

You are a member of staff on the Intensive Care Unit (ICU) and have just arrived to take over from the night team. Overnight there was a cardiac arrest on the ward and the night team are debriefing.

The team are discussing **Mr Lungs** - a 60M admitted for septic shock who had been on a ventilator for three days. Overnight the following occurred:

- **0200am:** While ventilated with an FiO2 of 50%, a Vt of 430 mL, Mr Lungs SpO2 suddenly dropped from 97% to 85%. **Nurse Cyber** increased the FiO2 to 100% but the patient continued to have SpO2 at 82%. [1]
- **Dr Vent** (the ICU doctor) assessed the patient and noticed that noticed that the ventilator displayed pressure and flow curves usually observed in pressure support mode (fixed pressure and decelerating flow), while it was still set in volume-controlled mode. **Dr Vent** reset the settings, confirming that the ventilator was still in volume-controlled mode.
- While doing this, the patient's SpO2 dropped further, leading to hypoxic bradycardia and asystole. The patient was revived following the prompt withdrawal of the endotracheal tube, the provision of manual ventilation via bag and mask, and a brief cardiac massage. The patient was then placed back on the ventilator.

The team were now discussing what caused the event and **Dr Vent** (the ICU registrar) states that she believes that **Nurse Cyber** must have changed the ventilator mode from volume-controlled to pressure support. **Nurse Cyber** states that he did not do this, however he raises his concern that the ventilator might be faulty as he heard about a series of ventilators with closed-loop systems harming patients in France, and that their systems are vulnerable to cyberattacks [1-2].

While the staff are discussing these events, a nurse calls for assistance at the end of the ward as another patient - **Mrs Chest**, has developed respiratory distress and is desaturating to SpO2 70%. **Mrs Chest** (a 55F) was initially put on a ventilator due to respiratory failure relating to SARS-Cov-2 induced acute respiratory distress syndrome [1].

You attend to **Mrs Chest** and notice that this ventilator is also displaying inconsistent settings – the pressure and flow curves suggest that the ventilator is in pressure support mode, yet analysis of the settings states it is in volume-controlled mode.

PETRAS

Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

You must form a management plan for Mrs Chest and for the other 10 patients on ICU who are all on the same type of ventilator.

Case-specific questions

1. Which systems in Emergency and Intensive Care may be vulnerable to technical malfunctions and/ or cyberattacks, and how might this manifest in patient illness?
2. What are the risks of closed-loop life support systems and medical systems based on Artificial Intelligence (AI) in acute medical settings?
3. If the patient had died, what are the appropriate post-mortem investigations and how should the cause of death be registered?
4. What measures and protocols are taken (by you or the hospital) to ensure the connected devices you are using are safe and performing accordingly?
5. Do you have concerns about the reliability of AI-based or automated medical devices? If so, how does this impact your clinical decision-making and professional responsibility?

General questions

1. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, devices, machinery, and/ or systems?
2. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?
3. What challenges do clinicians face when using medical software and/ or (quasi-)autonomous systems in patient care?

References

1. Dufour, Nicolas, et al. 'When a Ventilator Takes Autonomous Decisions without Seeking Approbation nor Warning Clinicians: A Case Series'. International Medical Case Reports Journal, vol. 13, 2020, pp. 521–29. PubMed, https://doi.org/10.2147/IMCRJ.S266969.

2. Eliash, Carmel, et al. 'SEC-C-U: The Security of Intensive Care Unit Medical Devices and Their Ecosystems'. IEEE Access, vol. 8, 2020, pp. 64193–224. IEEE Xplore, https://doi.org/10.1109/ACCESS.2020.2984726.

3.Chalvignac, Philippe. Breathing Assistance Apparatus. CA2520326C, 22 Jan. 2013, https://patents.google.com/patent/CA2520326C/en.

4. Sakiewicz, Paul G., et al. 'Abnormal Electrical Stimulus of an Intra-Aortic Balloon Pump with Concurrent Support with Continuous Veno-Venous Hemodialysis'. ASAIO Journal, vol. 46, no. 1, Feb. 2000, p. 142. journals.lww.com, https://journals.lww.com/asaiojournal/Fulltext/2000/01000/Abnormal_Electrical_Stimulus_of_an_Intra_Aortic.31.aspx.

5. Dameff, Christian J., et al. 'Clinical Cybersecurity Training Through Novel High-Fidelity Simulations'. The Journal of Emergency Medicine, vol. 56, no. 2, Feb. 2019, pp. 233–38. ScienceDirect, https://doi.org/10.1016/j.jemermed.2018.10.029.

Scenario 6: Seizure outbreaks in epilepsy management apps

Scenario description
(Patients are references by age and sex, e.g., 60M = 60-year-old male)

You work at a General Practice (GP) and have just seen your first patient - **Miss Brain.** Miss Brain is a 17F who tells you she had a relapse in her epilepsy this week, having experienced seizures in the evenings the last two nights. Both seizures came on when she was sat in bed at home, and states she was doing little at the time besides scrolling on her phone and checking the support forum of her epilepsy management app. Miss Brain shares that she is worried as two of her friends in her epilepsy support group have also had seizure relapses this week, without a clear cause.

Miss Brain was first diagnosed with Epilepsy 10 years ago and has been well-controlled and seizure-free for the past 3 years while managed on Sodium Valproate. The patient reports feeling otherwise well in herself, she has been taking her medications regularly, and has not experienced any other symptoms. Additionally, she denies starting any new medications or OTC drugs. She has been regularly using her epilepsy self-management app to record her mood, her medication adherence, and to chat with her support group in the app chat forum. Without indication of another cause, you question whether Miss Brain's app use could have caused her symptoms. Miss Brain states that she does use the app regularly, but this has never caused her a problem in the past.

You are aware of the previous virtual assaults on epilepsy patients that have occurred online, including the harmful impact caused by hackers targeting epilepsy support forums with changes in screen brightness. You must come up with a management plan for Miss Brain and consider the wider population health implications of this case.

Case-specific questions

1. How may cyberattacks on medical applications affect patients who suffer from photosensitive conditions, including migraine and epilepsy? What other patient groups may be at risk?

2. If you are concerned about the safety and performance of these medical applications, when, and to whom, do you communicate these concerns?

3. Who could you report this case to and where could you seek advice?

PETRAS

Sponsored by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity

4. What measures and protocols are taken (by you or your practice) to ensure your concerns about patients interacting with potentially compromised medical apps are communicated and reported to the appropriate authorities/ entities?

General questions

1. What challenges do clinicians face when interacting with patients who use digital platforms and software as a medical device (SaMDs) to manage their conditions?

2. What challenges do clinicians face when dealing with the consequences of a cyberattack resulting in compromised digital records, medical devices (including apps), machinery, and/ or (automated) systems?

3. For outpatient care where remote services (i.e. cloud-based services) are increasingly used to monitor and tailor treatment regimes, how would compromises to these critical, yet externally managed, services affect patient care?

References

1. Poulsen, Kevin. 'Hackers Assault Epilepsy Patients via Computer'. Wired. www.wired.com, https://www.wired.com/2008/03/hackers-assault-epilepsy-patients-via-computer/. Accessed 16 Jan. 2023.

2. Denning, Tamara, Yoky Matsuoka, and Tadayoshi Kohno. 'Neurosecurity: Security and Privacy for Neural Devices'. *Neurosurgical Focus* 27, no. 1 (1 July 2009): E7. https://doi.org/10.3171/2009.4.FOCUS0985.

3. Busby, Mattha. 'Malicious Tweets Targeting Epilepsy Charity Trigger Seizures'. The Guardian, 15 May 2020. The Guardian, https://www.theguardian.com/society/2020/may/15/malicious-tweets-targeting-epilepsy-charity-trigger-seizures.

4. South, L., & Borkin, M. (2020, October 23). Ethical Considerations of Photosensitive Epilepsy in Mixed Reality. https://doi.org/10.31219/osf.io/y32td

5. Alzamaman et al. (2021) 'Self-Management Apps with People with Epilepsy: Systematic Analysis'. JMIR Mhealth Uhealth. 2021 May; 9(5): e22489. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8196364/