“99.9% of clinicians wouldn’t expect a device to fail”: Insights from a clinically orientated workshop on healthcare cybersecurity and medical technology

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

Submitted to: Journal of Medical Internet Research
on: July 03, 2023

Table of Contents

“99.9% of clinicians wouldn’t expect a device to fail”: Insights from a clinically orientated workshop on healthcare cybersecurity and medical technology

Isabel Straw[1] MPH, BMBS, BMedSci, MSc; Irina Brass[1]; Andrew Mkwashi[2]; Inika Charles[1]; Amelie Soares[1]; Caroline Steer[1]

[1]University College London London GB
[2]Newcastle University Newcastle GB

Corresponding Author:
Isabel Straw MPH, BMBS, BMedSci, MSc
University College London
250 Euston Road
London
GB

Abstract

Background: Healthcare professionals receive little training on the digital technologies that their patients rely on. Consequently, practitioners may face significant barriers when providing care to patients suffering from digitally-mediated harms (e.g., device failures, medical cybersecurity exploits). Here, we explore the impact of technological failures in clinical terms.

Objective: Our study explored the key challenges faced by frontline healthcare workers during digital events, identified gaps in clinical training and guidance, and proposes a set of recommendation for improving digital clinical practice.

Methods: A qualitative study involving a one-day workshop of fifty-two participants, internationally attended, with multi-stakeholder participation. Participants engaged in table-top exercises and group discussions focused on medical scenarios complicated by technology (e.g., malfunctioning ventilators, malicious hacks on healthcare apps). Extensive notes from five scribes were retrospectively analysed and a thematic analysis was performed to extract and synthesise data.

Results: Clinicians reported novel forms of harm related to technology (e.g., geofencing in domestic violence, errors related to interconnected foetal monitoring systems) and barriers impeding adverse event reporting (e.g., time constraints, post-mortem device disposal). Challenges to providing effective patient care included a lack of clinical suspicion for device failures, unfamiliarity with equipment, and an absence of digitally tailored clinical protocols. Participants agreed that cyberattacks should be classed as Major Incidents, with the repurposing of existing crisis resources. Treatment of patients was determined by the role technology played in clinical management, such that those reliant on potentially compromised laboratory or radiological facilities were prioritised.

Conclusions: Here, we have framed digital events through a clinical lens, described in terms of their end-point impact on the patient. In doing so, we have developed a series of recommendations for ensuring responses to digital events are tailored to clinical needs and centre patient care. Clinical Trial: N/A

(JMIR Preprints 03/07/2023:50505)
DOI: https://doi.org/10.2196/preprints.50505

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

“99.9% of clinicians wouldn’t expect a device to fail”: Insights from a clinically orientated workshop on healthcare cybersecurity and medical technology

Isabel Straw[1]*, Irina Brass[1], Andrew Mkwashi[2], Inika Charles[1], Amelie Soares[1], Caroline Steer[1]

1. UCL Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London, UK
2. Newcastle University, Newcastle-upon-Tyne, UK
*Corresponding author (rmhiist@ucl.ac.uk)

Word count = 3490

AUTHOR STATEMENT

The authorship contributions are listed as per the CRediT authorship criteria: Conceptualization: IS, IB and AM.; Data curation: IS, IB, IC, AS, CS; Formal analysis: IS, IB, IC, AS, CS; Investigation: IS, IB, AM, IC, AS, CS; Methodology: IS, IB, AM; Resources: IB, AM; Supervision: IB; Validation: IB; Writing—original draft: IS; Writing—review and editing: IS, IB. All authors reviewed and approved the final version. Please also find the details of the researchers below, as per the COREQ (COnsolidated criteria for REporting Qualitative research) Checklist.

At the time of the research study and qualitative data collection: IS (female) was a medical doctor and PhD Candidate in Artificial Intelligence-Enabled Healthcare at University College London (UCL); IB (female) was an Associate Professor of Regulation, Innovation and Public Policy in the Department of Science, Technology, Engineering and Public Policy (STEaPP) at University College London; AM (male) was a Research Fellow on the Regulation and Standardization of Connected, Intelligent Medical Devices (REG-MEDTECH) project in the Department of Science, Technology, Engineering and Public Policy (STEaPP) at University College London; and IC (female), AS (female), and CS (female) were candidates on the Masters in Public Administration (MPA) in Digital Technologies and Policy at University College London and employed as Research Assistants on the REG-MEDTECH project.

FUNDING

This research is funded by the PETRAS National Centre of Excellence in IoT Systems Cybersecurity (EPSRC grant number EP/S035362/1).

ACKNOWLEDGMENTS

The authors would like to express their appreciation to the PETRAS team and all stakeholders who took part in our primary research and provided us with a wealth of information on this topic. Special thanks go to our project partners at BSI (the UK’s National Standards Body) for their guidance and support throughout this project, especially to Rob Turpin, Paul Sim, Emma Glass, and Matthew Chiles.

DATA AVAILABILITY

The clinical scenarios and relevant background research that was used to create the workshop content are available in the supplementary material.

Abstract

Background

Healthcare professionals receive little training on the digital technologies that their patients rely on. Consequently, practitioners may face significant barriers when providing care to patients suffering from digitally-mediated harms (e.g., medical device failures, cybersecurity

exploits). Here, we explore the impact of technological failures in clinical terms.

Objective
Our study explored the key challenges faced by frontline healthcare workers during digital events, identified gaps in clinical training and guidance, and proposes a set of recommendation for improving digital clinical practice.

Methods
A qualitative study involving a one-day workshop of fifty-two participants, internationally attended, with multi-stakeholder participation. Participants engaged in table-top exercises and group discussions focused on medical scenarios complicated by technology (e.g., malfunctioning ventilators, malicious hacks on healthcare apps). Extensive notes from five scribes were retrospectively analysed and a thematic analysis was performed to extract and synthesise data.

Results
Clinicians reported novel forms of harm related to technology (e.g., geofencing in domestic violence, errors related to interconnected foetal monitoring systems) and barriers impeding adverse event reporting (e.g., time constraints, post-mortem device disposal). Challenges to providing effective patient care included a lack of clinical suspicion of device failures, unfamiliarity with equipment, and an absence of digitally tailored clinical protocols. Participants agreed that cyberattacks should be classed as Major Incidents, with the repurposing of existing crisis resources. Treatment of patients was determined by the role technology played in clinical management, such that those reliant on potentially compromised laboratory or radiological facilities were prioritised.

Discussion
Here, we have framed digital events through a clinical lens, described in terms of their end-point impact on the patient. In doing so, we have developed a series of recommendations for ensuring responses to digital events are tailored to clinical needs and centre patient care.

Conflict of interest
The authors declare no conflict of interests.

Introduction

The unwell patient who seeks medical care due to a medical device fault, cybersecurity exploit, or failure in digital health infrastructure may encounter a clinical team who lack an understanding of the nature of their condition [1–7]. These digital events are often framed as computing issues, yet in practice they manifest as patient symptoms and signs and pose significant challenges to the treating clinicians at point-of-care (POC) [1-9]. In our digitised society, where healthcare provision is increasingly reliant on technological infrastructure, the ‘Internet of Medical Things’ (IoMT), and connected and intelligent medical devices, computing issues are increasingly translating into clinical complaints [2-8,10–16].

The Landscape of Digital Health Technologies

The proliferation of digital technologies in the healthcare sector has accelerated over the

past decade, with new medical devices entering the market, the growth of consumer health technologies, and the introduction of novel digital tools to hospital workflows (e.g. cloud-connected care platforms, digital assistants, remote monitoring) (10-12,17–22). These devices are connected to communication networks and the Internet to send, store, and process data in the cloud, forming integral components of the evolving 'Internet of Things (IoMT)' [10-12,21,23]. A subset of medical devices comprise standalone software, known as Software as a Medical Device (SaMD), which may incorporate varying degrees of Artificial Intelligence (AI) approaches and locked or adaptive machine learning (AIaMD) [10,17,25]. These novel digital tools present many oppurtunities for improving patient care, yet they have also introduced new vulnerabilities into the healthcare system that may impact patient safety [10,16,21,25-29].

New Risks in the Digital Health Landscape

Our increased reliance on digital infrastructure opens us up to new digital risks, exemplified by the increasing number of cyberattacks affecting the healthcare sector [2,26–29]. Borycki and colleagues have provided an overview of the new types of technology-induced errors that have arisen in the healthcare system with the introduction of health information technologies (HIT) [30]. The authors detailed the dangers of an overreliance on technology and explore the specific challenges faced by clinicians who are 'digital natives', including unrealistic expectations towards fault tolerance and the availability of digital systems [30-31]. Sax and colleagues consider the potential patient harm associated with a range of IT failures including loss of system availability, loss of data and loss of data integrity [31]. Alemzadeh and colleagues place technological events in their clinical context, linking adverse computer incidents to end-point clinical symptoms, uncovering a range of safety-critical computer failures that have resulted in significant patient harm and death [32].

In the UK, the retrospective analyses of the NHS WannaCry attack highlighted the importance of cybersecurity for patient safety, yet many NHS hospitals still lack guidance regarding the incident response to a cyberattack [29]. Furthermore, security researchers have sounded the alarm regarding the potential for individual-level healthcare attacks termed 'MedJacking', referring to the remote manipulation of patient's medical devices such as insulin pumps and deep brain stimulators [6,33]. When such adverse events occur, research has described the challenges encountered by clinicians for whom the clinical manifestations of technological failures may be unfamiliar [1,5,15]. A recent review of patient illnesses stemming from digital technologies - termed 'Biotechnological syndromes' - detailed a range of clinical presentations relating to implanted medical devices (e.g., complications of neurostimulators) and technologies within the wider healthcare system (e.g., harms from failures in drug delivery systems) [5].

Clinical complications may also arise from digital technologies not traditionally thought of as 'digital health' technologies. In particular, the rise in Biohacking technologies has presented unexpected challenges to clinicians described by Fram and Colleagues in their review of the clinical considerations of consumer implants and microchips [7, 34]. Clinical presentations may also be affected by technology through unexpected mechanisms, highlighted in cases of technology-facilitated abuse in healthcare settings [35-36]. Research from the Domestic Violence field has described the harms faced by patients encountering technology-facilitated abuse (e.g. harm inflicted through the manipulation of smart devices) and the need for clinicians to update safeguarding protocols to encompass these risks [35-36].

The introduction of healthcare AI has brought forward novel ethical questions regarding accountability and liability, with researchers raising concerns about the removal of the 'human-in-the-loop' in clinical systems that embed autonomous functions [10,27]. Habli and colleagues discuss the challenges of determining moral accountability in complex socio-technical systems involving AI software, and Fahrud and Zokaei frame these challenges through the traditional pillars of medical ethics (autonomy, beneficence, nonmaleficence, and justice) [37-38]. Lee and colleagues highlight the potential clinical dangers of autonomous systems in their report that describes several cardiac arrests stemming from algorithmic errors in a series of ventilators [39]. In addition to concerns surrounding AI autonomy, ethicists have illuminated further issues associated with these technologies, including risks of bias and discrimination in AI-supported clinical decision tools [40-43].

Clinical Medicine and Digital Health Risks

Currently, clinicians receive little training on the emerging digital technologies that their patients rely on for care and that professionals depend on to perform their work [1-8, 15]. As detailed by Sally Adee in her comprehensive history of the life sciences and physical sciences, the separation of these two scientific domains over the past 200 years has resulted in distinct professional languages and expertise, which often struggle to understand one another [44]. However, with the advance of bio-digital convergence and the growing prevalence of digital health technologies, clinicians are increasingly likely to encounter patients that are no longer purely biological but rely on varied digital devices requiring an understanding of the physical sciences [5, 44-45]. Furthermore, the government bodies tasked with overseeing digital health technologies have faced the challenge of understanding biomedical innovations arriving from overseas, requiring an alignment of domestic standards with the global market [10,24-25]. As a result, the technologies that play a key role in shaping a patient's journey may be poorly understood by the healthcare practitioners and the governmental agencies responsible for public oversight.

Research Aim

The disciplines of clinical medicine, cybersecurity and engineering have long operated in silos and as a result we lack effective frameworks for patients whose health complaints emerge from the intersection of these domains. In this article we present the findings of a confidential multi-stakeholder workshop that bridged the gap between these professions, facilitating an interdisciplinary discussion on the key challenges affecting digitally-dependant patients. We provide insights from frontline staff on the difficulties faced during digital events (e.g. cyberattacks, device failures), detail differing perspectives from varied stakeholder groups, and present a series of recommendations for ensuring best clinical practice in the evolving digital healthcare infrastructure.

Methods

The workshop titled *"Emerging Digital Technologies in Patient Care: Dealing with connected, intelligent medical device vulnerabilities and failures in the healthcare sector"* took place at Goodenough College, London in the United Kingdom (UK) in February 2023. The workshop was part of an EPSRC-funded project investigating how healthcare systems, regulations, and standards are responding to the cybersecurity and algorithmic integrity challenges posed by the growing use of connected and intelligent medical devices.

Participant recruitment and ethical considerations

The workshop of fifty-two participants had representation from the European Union, the

United Kingdom, and the United States of America (USA), involving a wide range of stakeholder groups (Table 1). Ethical approval no 222137/001-0023A was obtained from the UCL Research Ethics Committee.

All workshop participants were recruited based on their practical experience and expertise in digital healthcare. Limited snowball sampling was used to identify practitioners and experts in the field. Participants were recruited via email by the research team, leveraging the academic, clinical, and professional networks of IS, IB and AM and their affiliated institutions. Thus, participants were aware of the researchers' academic profiles prior to the workshop and were provided with detailed information in advance describing the goals of the research. A participant information sheet detailing the research project and a consent form were circulated in advance, and participants were asked to return the consent form via email. All participants provided written informed consent for their contributions to be used as anonymised research data.

No patient or healthcare data was used for the workshop and all scenarios (Table 2) were fictitious and informed by published research. Workshop discussions were held under the Chatham House Rule and neither the identity nor the organisational affiliation of participants will be disclosed in research outputs derived from the workshop. Participants were identified solely by broad stakeholder category (Table 1) using different badge colours for note taking purposes. No compensation was provided to workshop participants.

Table 1: Details of workshop participants and their disciplinary backgrounds
Categories of stakeholders who participated in the workshop

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**

Workshop structure

The workshop consisted of two parts: (i) a series of expert talks followed by Q&A & group discussion, & (ii) breakout table-top exercises in which participants discussed and designed a response to a clinical scenario complicated by technology (Table 2). Clinical scenarios were written to account for the diversity of healthcare technologies and the disciplinary backgrounds represented in the room. All scenarios were based on published case reports and reported issues related to digital health technologies. The full case scenarios are provided in the supplementary material and detailed in the online workshop description [46]. Notetakers were present throughout the workshop to record details of Q&A sessions, group discussions and table-top exercises (audio and visual recording was not used). Notetakers received in-person training in advance of the workshop, to review the research materials, discuss the scenarios, address any questions, and agree on a framework for the data

collection process.

Table 2: Details of the clinical scenarios designed for table-top exercises specific to different specialities, all of which are based on published case reports (46).

Clinical Speciality	Clinical scenario for table-top discussion
Acute Medicine	**"Caring for medical patients during a weekend cyberattack":** In Scenario 1 a hospital cyberattack compromised a (i) cloud-based platform that detailed chemotherapy regimens for oncology patients, (ii) smart drug-delivery systems within the hospital, and (iii) patient electronic health records (EHRs). The patients described within the scenario all required specific dosing of medications and careful fluid management, the group had to prioritise patients for care and design a wider hospital response.
Acute Medicine	**"Managing unwell patients during a cyberattack on the acute medical unit (AMU)":** Scenario 2 focused on clinical cases requiring careful management of acid-base conditions that necessitated effective blood gas analysis (diabetic ketoacidosis, renal failure) and attentive fluid management (decompensated heart failure), however the laboratory, blood gas machine and smart pumps were all compromised.
Acute Medicine	**"Treating blind – Patient care during a radiological cyberattack":** Scenario 3 focused on patient conditions where clinical decision-making relied on radiological information, including (1) Identification of pneumothorax for chest drain insertion, (2) Use of chest Xray to confirm position of nasogastric tube, (3) MRI imaging to diagnose cauda equina syndrome and (4) CT imaging to identify an intercranial bleed. In the scenario the Electronic Health Record (EHR) system was unavailable, and the radiological imaging system was known to be compromised (although the impact on the integrity of scans was unclear).
Surgery & Obstetrics	**"Mother, baby and spinal cord stimulator":** In Scenario 4 the team needed to decide on the best management for a pregnant patient presenting with signs of labour, who reported having a closed-loop spinal cord stimulator in situ. The patient is likely to need a caesarean section due to the breech position of the baby but has not had a preanesthetic evaluation and there is no available information regarding the spinal cord stimulator. The model of spinal stimulator has AI-integrated functionalities, including the self-adjustment of settings based on patient posture. The team must design a safe clinical care plan that accounts for the device and any complications.
Emergency and Intensive Care	**"Patient care and ventilator autonomy":** Scenario 5 was based on the Intensive Care Unit (ICU), where a ventilator malfunction causes patients to go into cardiac arrest. The

	ventilators have integrated automated functions that allow them to update their own settings, however the attending clinicians are unable to interpret the settings of the machine. The team were tasked with determining the immediate clinical response and discussing the wider implications of closed-loop life support systems in critical medical settings.
General Practice	**“Seizure outbreaks in epilepsy management apps”:** In Scenario 6 a teenager presents to her General Practitioner (GP) with a relapse in seizure symptoms, having a known diagnosis of epilepsy that had been previously well controlled. It is suggested that the epilepsy management app on her phone has been compromised. The team were tasked with planning an appropriate response for this patient and the wider population health implications.

Research data analysis

Extensive notes taken during the workshop were retrospectively analysed and the data from the five note-takers was cross-referenced to ensure consistency in the reported results. Four of the researchers coded the qualitative data and undertook an inductive thematic analysis to extract major and minor themes present within the text. Anonymised examples of clinical cases involving technology provided by clinicians were collected as use cases and described in the results.

Results

Our results are divided into themes extracted from panels Q&As and group discussions (Section 3.1), and those identified from the breakout exercises on different clinical scenarios (Section 3.2).

Group discussions: Identified themes

(i) Digital infrastructure: *“The hospital still has Windows 10”*

The outdated IT infrastructure of the National Health Service (NHS) in the UK is a known risk for cyberattacks, as these systems can more easily be exploited by malicious actors [26-29, 46-47). Participants described the compounding effect that poor IT infrastructure has on their digital behaviour, which may further exacerbate the risk of cyber-exploitation. For example, the fact that IT systems are often slow, break, or are unreliable result in clinicians sharing computers, Logins and engaging in risky cyber-hygiene practices. Additionally, the current pressure on NHS Staff due to underfunding and staff shortages results in a lack of capacity for additional training on cybersecurity.

Clinicians shared that it was hard to get excited about the introduction of digital systems when the basic healthcare needs of their patients were not being met. Further, practitioners shared concerns regarding the impact of digital innovation on healthcare inequalities, as access to newer technologies is often mediated by wealth therefore deepening socioeconomic disparities in health outcomes. We heard examples of tech-poverty affecting patients, including accessibility issues related to the rise in telehealth which is inaccessible to disadvantaged patient groups. Clinicians also raised concerns regarding technology-facilitated abuse, with one participant describing the malicious use of GPS tracking technologies to ‘Geofence’ young women and girls within specific city boroughs, such that abusive parties would receive notifications if they left defined geographic areas (Table 3).

(ii) Trust & medical devices: *"The device should be considered guilty until proven otherwise"*

Clinicians expressed concerns regarding the often-unchallenged assumption that exists in the medical community regarding device functionality, with one practitioner sharing the view that *"99.9% of clinicians wouldn't expect a device to fail",* reinforced by peers stating that they'd be highly unlikely to suspect an embedded technology as a source of pathology. In cases where medical devices do fail, manufacturers shared that it is not always easy to identify the cause. Companies may be able to take a piece of technology back and attempt to replicate the failure mode, however often these faults are attributed to unknown internal or external factors.

Manufacturers highlighted the risk of eroding patient trust when device malfunctions are poorly communicated, detailing historic challenges that they have faced when communicating issues to patients, stating *"It is easy to spend millions on recalls when it is not necessary".* Workshop participants discussed that manufacturers are often cognisant that technologies fail, but may feel that publicising all of these events could cause unnecessary alarm, especially in cases where a fault (e.g., software bug) is likely inconsequential but causes fear due to its presence in a consequential technology (e.g. a ventilator). Lastly, representatives from the policy domain highlighted the potential for fake news and disinformation that could result from misinterpreted reports of technological failures. Participants also raised issues of public vs. private interests, exploring the role that financial incentives play when making decisions regarding device fault disclosures.

(iv) Responsibility and Liability: *"Clinicians don't have time to report this"*

Views differed between clinicians and manufacturers on the topics of device failure reporting, post-market surveillance and professional liability in cases of patient harm. Clinicians shared frustrations that they *"don't have time to report this"* (referring to device malfunctions), stating that responsibility for consistent surveillance of deployed devices should be with the manufacturer. The issue of transparency was evident when discussing the communication between clinicians, manufacturers and regulatory agencies, as manufacturers often found themselves limited in the information they could share due to commercial confidentiality. Furthermore, there was confusion as to whether reporting device errors was mandatory, with clinicians stating that this was a voluntary (and unfortunately often underperformed) action, and other participants stating this was an obligation.

Workshop participants heard from representatives from the consumer implant industry, who described the increasing uptake of implanted RFID and NFC Chips in younger generations. Such body modification technologies that are sited under the skin can cause medical complications (e.g. infections, soft tissue injury), however these technologies do not fall under medical device regulation. It manifested that members of the public occasionally approach these companies' expressing fears of being chipped by 'the government' or 'aliens', yet in the case of potentially serious mental health concerns these individuals are not redirected to appropriate healthcare support. Additional ethically contentious cases were discussed including requests from family members to 'chip' older relatives with dementia, or younger children. There was a clearly identified need for improving safeguarding referral pathways.

Clinical Scenarios

The focused disciplinary table-top exercises facilitated a deeper dive into the specific

clinical issues that may arise within each clinical domain.

(i) Medical Scenarios – *"With most tech we don't know how it works so we don't know how to trust it"*

The three hospital-based medical scenarios described failures in cloud-based treatment platforms, laboratory equipment, radiological systems, and electronic health records. Clinicians initially drew parallels to previous experiences where IT had been compromised referencing the WannaCry 2017 attack and climate events (e.g. heatwaves) affecting computer systems. Practitioners described the chaos of shifting to paper-based prescribing and note-taking during on-call and overnight hours, during which time they noted a lack of leadership and defined protocols for responding to the event clinically.

In designing their response, all groups reached consensus that the cyberattack should be classed as a "*Major Incident",* activating a chain of responses including the recruitment of additional staff, awareness at the national level, communication across sites, an effective PR response, and allocation of roles to those with sufficient skills and seniority. Senior team members suggested the development of battle-bags and action cards that are commonly used in other Major Incident events, citing Grenfell Tower and the Manchester Bombing as examples. Clinicians demonstrated some awareness of available resources, including NHS Digital and Chief Information Officers, however these resources were relatively unheard of within the groups.

The scenario suggested there were cybersecurity vulnerabilities in the drug-delivery and laboratory systems present on the wards, to which healthcare staff reported a preference for shutting down technology entirely as a safety measure (while acknowledging that this could be unnecessary and cause delays and even more harm). When discussing plans to turn off digital systems, the groups shared their concerns about what disabling devices would do and whether there was a default safe mode that could protect patients. In shutting down digital equipment, participants decided to return to rudimentary clinical techniques including dripping (the act of delivering intravenous medications based on drips of liquid). The teams raised concerns for younger generations of clinicians who may not have this non-digital foundation to fall back on.

Lastly, practitioners identified the patients most at risk of harm in the context of IT manipulation in the hospital and developed a clinical hierarchy specific to digital threats. The patients with diabetic ketoacidosis and cauda equina were identified as likely to suffer the worst outcomes due to the reliance on laboratory and radiological resources for treatment. By prioritising the patients according to the role that technology played in their clinical management, participants framed the cyberattacks in clinical terms.

(iii) Surgical Scenario – "Mother, baby and spinal cord stimulator" – "There is no way of knowing how the body is communicating with the device"

The surgical group was tasked with managing a patient in active labour who had a potentially compromised implanted spinal cord stimulator. Through the discussion it became apparent that there was lack of clinical knowledge regarding the implications of the technology, and the healthcare staff opted to focus on the medical management that they did understand while putting the technical components to one side. In discussing the follow up to the case, standards body representatives raised concerns that the incident would not be flagged as an adverse outcome, supported by clinicians who indicated that this would be unlikely to be reported.

(iii) Emergency and Intensive Care Scenario – "Patient care and ventilator autonomy"
The clinicians first drew comparisons to historic crises events including the 1952 Copenhagen crisis in which medical students were recruited to manually ventilate patients [49]. When discussing the initial response to the scenario, the team discussed disconnecting all patients from the ventilators, while acknowledging the challenges of doing this in an ICU where patients are dependent on life support systems. The group discussed the specific implications of AI and closed-loop systems within the medical equipment, identifying the central issue of trust and a lack of understanding of the technological mechanisms. The lack of training in AI systems was felt to be compounded by the absent training regarding cyberattacks, with clinicians sharing that they had *"never had a training day on what would happen in this scenario".*

(iii) Community Care and General Practice (GP) Scenario – "Seizure outbreaks in epilepsy management apps"
The scenario based in community care described a teenage patient who experienced a relapse in seizure symptoms, suspected to be related to a malicious hack on an epilepsy app. The group began by identifying possible adverse health effects including seizures, headaches, distress, loss of vision, loss of focus, visual effects, and airways compromise. At-risk patient groups were noted, including dementia patients and those with neurodiversity. For immediate clinical management, practitioners felt that staff were likely to tell the patient to avoid the app or their phone entirely, reiterating a theme heard in the other groups of completely disconnecting from the technology.

In contrast to the other groups, the GPs discussed reporting the case to the police and ministry of defence, due to the concern of a malicious attack and the implications this could have for a large number of people using the app. Participants also described the need to involve parents as this was a paediatric case, and the role of the app company in protecting their users.

Uncovered Examples
During the workshop practitioners provided anonymised anecdotes of patient harm where technology played a role. Table 3 provides these example cases. In reflecting on a patient death, one participant discussed the lack of post-mortem guidance, highlighting that the disposal of devices as medical waste precludes the evaluation of their involvement in a death.

Table 3 Anecdotes and examples of patient presentations related to technology that were disclosed by participants at the workshop

Medical Domain	Quote from Participant
Hospital Medicine	In a case of a malfunctioning piece of radiological equipment, we had a case where three dozen patients were exposed with higher doses, above the diagnostic reference level.
	We know we have issues with pacemaker batteries, but we don't know how many are affected. We need to understand how to manage that risk.
	Women who was a 35 year-old, diabetic patient who died and it was a surprise to the clinical team. The patient had been on a pump and the clinician discussed with the coroner if the pump could have

	contributed? The husband had thrown the insulin pump in the bin, no-one had looked at it so there was no clear cause. We need to collect devices after a death, maybe give them to the police.
Surgery	In Obstetrics and Gynaecology, there was a case of the wrong women being given an Emergency C-Section because the communication lines from two foetal CTGs overlapped, and one baby's readings had been assigned to the wrong mother.
Community Care	In GP surgery, Apple watches causing patients to think their heart rhythms are abnormal.
	Seen issues in General Practice with tech-abuse & GPS tracking. Young girls in some communities have to stay inside their borough, otherwise an alarm goes off to their family/partner.

Discussion

In a patient journey, the individual is likely to encounter various forms of technology, from their electronic health record (EHR), to advanced, interconnected, automated and intelligent healthcare technologies [15,46, 50-51]. In these journeys, healthcare staff are the immediate point of contact when clinical care goes wrong, and patient health deteriorates [1-5]. In this article we have explored the points of digital vulnerability that may contribute to patient illness along these trajectories, and have discussed the issues of cybersecurity, device failures and faulty AI systems from the perspective of the treating clinicians.

Clinicians from a diverse range of specialties responded in a similar manner when confronted with failures in digital devices, opting to immediately shut down the technology. Whether this was disconnecting patients from ventilators, disabling all medication smart pumps, or advising patients to turn off phones that were vulnerable to malicious hacks - the safest measure was often considered to be preventing any ongoing interaction between the technology and the patient's physicality. The response is understandable given that clinicians receive little education on these tools and do not trust the systems or have the confidence to appropriately evaluate them.

Yet when clinicians are not informed of a potential technological failure, the default position appears to be the opposite and to trust devices entirely, such that *"99.9% of clinicians wouldn't expect a device to fail"*. Hence, an interesting dichotomy exists – when a clinician hasn't been given reason to doubt a device, they will often trust the device over the patient (e.g., believing the patient's blood glucose data, as opposed to their subjective symptoms), however once doubt is introduced the clinicians opt to disregard the technology completely. The polarity of these reactions mirrors the black and white nature of the black-box technology that remains opaque to clinicians using the digital tools. This delicate relationship reinforces the importance of effective communication around medical device failures with clinicians as well as with the public.

The lack of reporting regarding digital adverse events is a regulatory and public policy concern. Table 3 provides a list of events we collected in this workshop, of which several remained unreported and describe significant patient harm. Within these stories we heard new examples of biotechnological syndromes and forms of technology-facilitated abuse that add to the existing literature reporting issues of technology in domestic violence and the risks posed to vulnerable patients [5, 35-36].

We heard differing opinions on where responsibility and professional liability should lie

when patient harm occurs because of a technology malfunctioning, with clinicians sharing the view the manufacturers are responsible for ongoing follow-up and manufacturers stating that clinicians are responsible for the outcomes of patients with embedded devices. Healthcare professionals advocated for a higher standard to be placed on manufacturers with regards to patient trust and transparency, citing parallels to the Hippocratic oath and fundamental medical ethics taught in medical school. These suggestions have previously been made by several healthcare cybersecurity researchers who developed a “Hippocratic Oath for Connected Medical Devices” [41–43].

Conclusion

Our research has taken the unique approach of positioning digital healthcare technology failures in their medical context, viewed through the lens of the clinician at point-of-care. In doing this, we demonstrate how healthcare staff can form tailored clinical hierarchies when faced with healthcare cyberattacks, such as prioritising patients’ dependant on digitally vulnerable systems (e.g. spinal injuries requiring radiological imaging) or identifying at risks groups of mobile screen-based hacks (e.g. epilepsy, neurodiverse, and dementia patients). Understanding cyberattacks as clinical attacks in this manner provides an opportunity to form the guidelines and major incident response protocols that our participants identified as an urgent and lacking resource in hospital settings.

Our findings illustrate gaps in clinical knowledge regarding medical technology and a lack of confidence in managing these scenarios that can only be addressed with improved clinical education and training. To ensure effective patient care in our environment of evolving digital infrastructure, historic IT responses to cyberattacks and device failures must be married with the clinical needs and perspectives provided in this report. Our research shines a light on a critical and understudied area at the intersection of clinical medicine and digital health, that requires greater research and professional guidance. We provide a series of recommendations based on our findings:

Recommendations:

1. **Hospital Protocols and Incident Plans:** Cyberattacks should be treated as clinical attacks, framed similarly to other major incidents such as terrorist and extreme weather events [55]. To achieve this, cyberattack threat models should be developed with end-point clinical symptoms and signs in mind, necessitating input from clinicians and engineers. Hospitals and healthcare practices should develop Major Incident Protocols that specify the clinical steps to be taken in a cyberattack, hierarchically prioritising patient groups and repurposing existing resources such as action cards, dedicated response teams, battle-bags, and communication pathways for escalation.

2. **Medical Education and Clinical Training:** Healthcare practitioners require a fundamental understanding of the novel digital technologies that their patients rely on, in order to treat them effectively when digital complications arise. Software-based medical devices, especially those connected to communication networks and with AI integrated functionalities, require continuous monitoring of their performance by hospital staff and their medical device inventory teams. Digitally themed professional courses through the UK Royal Colleges would incentivise an uptake of this training, in addition to integrating educational content into NHS Trust mandatory training modules, clinical orientation and induction weeks in hospitals, and medical school

education curricula.

3. **Academia and Research:** Research focused on the health complications of digital technologies needs to advance at a parallel rate to the development and deployment of digital healthcare tools and devices. Future research focused on the symptoms and signs of digital failures and technological pathology would improve the ability of clinicians to diagnose these cases, and consequently report them to the appropriate bodies.

4. **Manufacturer Training and Support:** An easily accessible interface between manufacturers and clinicians is required, to ensure healthcare staff can find appropriate information about the performance of connected and intelligent medical devices in a timely manner. Manufacturers could develop “how to” cards and clinically tailored resources about their digital medical devices, which would be more useful to healthcare staff than traditional user manuals.

5. **Regulation and Reporting:** Increased interaction is needed between regulatory agencies, such as the MHRA, and clinical teams. Through events in medical schools, hospitals, and community healthcare practices, representatives of public and regulatory bodies may provide additional support to clinicians on the reporting processes and existing guidance regarding software-based and connected medical devices.

Limitations

While we engaged a range of critical stakeholders in our workshop, we were limited by sample size and the representativeness of our participants. In future research it would be beneficial to engage a wider range of clinical specialities, such as dermatologists, oncologist, radiologists and neurologists where digital health technologies are expanding rapidly. Furthermore, we have limited our focus to emerging digital technologies, with functionalities including telemetry, internet-connectivity and Artificial Intelligence (AI). As a result, we have not examined issues associated with static medical device, e.g., adverse reactions to materials used for hip implants.

References

1. 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. *PubMed*, https://doi.org/10.1016/j.jemermed.2018.10.029.

2. Dameff, Christian, et al. ‘Cyber Disaster Medicine: A New Frontier for Emergency Medicine. Annals of Emergency Medicine. Volume 75, issue 5, p642-647, May 2020. Doi: https://doi.org/10.1016/j.annemergmed.2019.11.011

3. Sommer M, Stiksrud EM, von Eckardstein K, Rohde V, Paulus W. When battery exhaustion lets the lame walk: a case report on the importance of long-term stimulator monitoring in deep brain stimulation. BMC Neurol. 2015 Jul 19;15:113.

4. Shao, Weiru. ‘Cochlear Implant Electrode Failure Secondary to Silicone Touch-up during Device Manufacturing’. Otology & Neurotology: Official Publication of the American Otological Society, American Neurotology Society and European Academy of Otology and Neurotology, vol. 34, no. 7, Sept. 2013, pp. e72-75. https://doi.org/10.1097/MAO.0b013e318298aaaf.

5. Straw, I., Rees, G. & Nachev, P. 21st century medicine and emerging biotechnological syndromes: a cross-disciplinary systematic review of novel patient presentations in the age of technology. BMC Digit Health 1, 41 (2023). https://doi.org/10.1186/s44247-023-00044-x

6. Adashi EY, Thomasian NM. Medical Devices in Harm’s Way: Medjacking. JAMA Health Forum. 2020 Jan 23;1(1):e200007.

7. Fram BR, Rivlin M, Beredjiklian PK. On Emerging Technology: What to Know When Your Patient Has a Microchip in His Hand. The Journal of Hand Surgery. 2020 Jul 1;45(7):645–9.

8. Straw I, Ashworth C, Radford N.

9. Guidance for manufacturers on reporting adverse incidents involving Software as a Medical Device under the vigilance system. UK Government. Accessed June 2023. Available from: https://www.gov.uk/government/publications/reporting-adverse-incidents-involving-software-as-a-medical-device-under-the-vigilance-system/guidance-for-manufacturers-on-reporting-adverse-incidents-involving-software-as-a-medical-device-under-the-vigilance-system

10. Mkwashi, Andrew and Brass, Irina, The Future of Medical Device Regulation and Standards: Dealing with Critical Challenges for Connected, Intelligent Medical Devices (September 7, 2022). PETRAS National Centre of Excellent in IoT Systems Cybersecurity: London (2022), DOI: 10.5281/zenodo.7054049, Available at SSRN: https://ssrn.com/abstract=4226057 or http://dx.doi.org/10.2139/ssrn.4226057

11. Pani S, Patra P, Ferrari G, Kraleva R, Wang X. The Internet of Medical Things: Enabling Technologies and Emerging Applications. In Instituteion of Engineering and

Technology (The IET). p. 2–4. Available from: https://air.unipr.it/handle/11381/2938191

12. Amato C. Internet Of Bodies: Digital Content Directive, And Beyond. Jipitec. 2021 May 18;12(2). Available from: https://www.jipitec.eu/issues/jipitec-12-2-2021/5285

13. South L, Borkin M. Ethical Considerations of Photosensitive Epilepsy in Mixed Reality. OSF Preprints; 2020. Available from: https://osf.io/y32td/

14. Sudden Death Associated with Severe Hypoglycemia in a Diabetic Patient During Sensor-Augmented Pump Therapy with the Predictive Low Glucose Management System. Novemver 2015. Available from: https://pubmed.ncbi.nlm.nih.gov/33462171/

15. Straw I, Dobbin J, Luna Reaver D, Tanczer L. 'Medical Cyber Crises and Biotechnological Syndromes: A Multisite Clinical Simulation Study Focused on Digital Health Complaints'. The Lancet, vol. 402, Nov. 2023, p. S88. ScienceDirect, https://doi.org/10.1016/S0140-6736(23)02082-2.

16. H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk and J. Raman, "Analysis of Safety-Critical Computer Failures in Medical Devices," in IEEE Security & Privacy, vol. 11, no. 4, pp. 14-26, July-Aug. 2013, doi: 10.1109/MSP.2013.49.

17. Ronte H. Medtech and the internet of medical things: How connected medical devices are transforming health care. Deloitte; Available from: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-%20Care/gx-lshc-medtech-iomt-brochure.pdf

18. Afolabi BA. Remote Monitoring of Patients with Implanted Cardiac Devices - A Review. 2012 Apr 8. Available from: https://www.ecrjournal.com/articles/remote-monitoring-patients-implanted-cardiac-devices-review

19. Nurshod A, Khujamatov K, Lazarev A. Remote Monitoring System Architectures in Healthcare. In: 2021 International Conference on Information Science and Communications Technologies (ICISCT). 2021. p. 01–5.

20. Tarakji KG, Zaidi AM, Zweibel SL, Varma N, Sears SF, Allred J, et al. Performance of first pacemaker to use smart device app for remote monitoring. Heart Rhythm O2. 2021 Oct;2(5):463–71.

21. Turpin R, Hoefer E, Lewelling J, Baird P. Machine Learning AI in Medical Devices: Adapting Regulatory Frameworks and Standards to Ensure safety and Performance. Association for the Advancement of Medical Instrumentation (AAMI), British Standards Institute (BSI).; 2020. Available from: https://www.bsigroup.com/en-US/medical-devices/resources/Whitepapers-and-articles/machine-learning-ai-in-medical-devices/

22. Garg, Shivank, et al. 'Clinical Integration of Digital Solutions in Health Care: An Overview of the Current Landscape of Digital Technologies in Cancer Care'. JCO Clinical Cancer Informatics, no. 2, Dec. 2018, pp. 1–9. DOI.org (Crossref), https://doi.org/10.1200/CCI.17.00159.

23. USA FDA. Artificial Intelligence and Machine Learning (AI/ML) - Software as a

Medical Device: Action Plan. USA: Food and Drug Administration (FDA); 2021 Sep.

24. Medical technology strategy. UK Government. Accessed May 2023. Available from: https://www.gov.uk/government/publications/medical-technology-strategy/medical-technology-strategy

25. Regulatory Horizons Council, UK Government. The Regulation of Artificial Intelligence as a Medical Device. November 2022. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120503/RHC_regulation_of_AI_as_a_Medical_Device_report.pdf (Accessed 27th November 2023)

26. Ghafur S, Grass E, Jennings NR, Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study. The Lancet Digital Health. 2019 May 1;1(1):e10–2.

27. Ghafur S, Fontana G, Martin G, Grass E, Goodman J, Darzi A. Improving Cyber Security in the NHS. London: Imperial College London; Available from: https://www.imperial.ac.uk/media/imperial-college/institute-of-global-health-innovation/Cyber-report-2020.pdf

28. Durkin M, O'Brien N, Ghafur S. Cybersecurity in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management. 2021 Mar 3;

29. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digit Med. 2019 Oct 2;2(1):1–7.

30. Borycki E et. al: Methods for Addressing Technology-induced Errors: The Current State. Yearb Med Inform. 2016 Nov 10;(1):30-40. doi: 10.15265/IY-2016-029.

31. Sax U et. al: The Rising Frequency of IT Blackouts Indicates the Increasing Relevance of IT Emergency Concepts to Ensure Patient Safety. Yearb Med Inform. 2016 Nov 10; (1):130-137. doi: 10.15265/IY-2016-038.

32. H. Alemzadeh, R. K. Iyer, Z. Kalbarczyk and J. Raman, "Analysis of Safety-Critical Computer Failures in Medical Devices," in IEEE Security & Privacy, vol. 11, no. 4, pp. 14-26, July-Aug. 2013, doi: 10.1109/MSP.2013.49.

33. Pycroft L, Boccard SG, Owen SLF, Stein JF, Fitzgerald JJ, Green AL, et al. Brainjacking: Implant Security Issues in Invasive Neuromodulation. World Neurosurg. 2016 Aug;92:454–62.

34. Gangadharbatla H. Biohacking: An exploratory study to understand the factors influencing the adoption of embedded technologies within the human body. Heliyon. 2020 May 1;6(5).

35. Straw I, Tanczer L. Safeguarding patients from technology-facilitated abuse in clinical settings: A narrative review. PLOS Digital Health. 2023 Jan 4;2(1):e0000089.

36. Tanczer LM, López-Neira I, Parkin S. ‘I feel like we’re really behind the game’: perspectives of the United Kingdom’s intimate partner violence support sector on the rise of technology-facilitated abuse. Journal of Gender-Based Violence. 2021 Oct 1;5(3):431–

37. Farhud DD, Zokaei S. Ethical Issues of Artificial Intelligence in Medicine and Healthcare. Iran J Public Health. 2021 Nov;50(11):i-v. doi: 10.18502/ijph.v50i11.7600. PMID: 35223619; PMCID: PMC8826344.

38. Habli I, Lawton T, Porter Z. Artificial intelligence in health care: accountability and safety. Bull World Health Organ. 2020 Apr 1;98(4):251-256. doi: 10.2471/BLT.19.237487. Epub 2020 Feb 25. PMID: 32284648; PMCID: PMC7133468.

39. Dufour N, Fadel F, Gelée B, Dubost JL, Ardiot S, Di Donato P, et al. When a ventilator takes autonomous decisions without seeking approbation nor warning clinicians: A case series. International Medical Case Reports Journal. 2020;13:521–9.

40. Straw I, Wu H. Investigating for bias in healthcare algorithms: a sex-stratified analysis of supervised machine learning models in liver disease prediction. BMJ health & care informatics. 2022;29(1).

41. Wu H, Sylolypavan A, Wang M, Wild S. Quantifying Health Inequalities Induced by Data and AI Models. 2022. p. 5192–8. Available from: https://www.ijcai.org/proceedings/2022/721

42. Obermeyer Z, Powers B, Vogeli C, Mullainathan S. Dissecting racial bias in an algorithm used to manage the health of populations. Science. 2019 Oct 25;366(6464):447–53.

43. Straw I. The automation of bias in medical Artificial Intelligence (AI): Decoding the past to create a better future. Artificial intelligence in medicine. 2020;110:101965.

44. We Are Electric: The New Science of Our Body's Electrome. 2023. Publisher: Canongate Books ; ISBN: 9781838853327 ; Number of pages: 352

45. Policy Horizons Canada. (2020). Exploring biodigital convergence: What happens when biology and digital technology merge? Canada: Government of Canada. 11 February. https://horizons.gc.ca/wp- content/uploads/2020/02/Biodigital-Convergence-with-Links-Final-02062020.pdf . Accessed 01 October 2023.

46. Brass I, Straw I, Mkwashi A, Charles I, Soares Mesquita A, Steer C. 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; 2023 Jun. Available from: https://zenodo.org/record/8011139

47. Sharma S. Outdated IoT healthcare devices pose major security threats. CSO Online. 2022. Accessed May 2023. Available from: https://www.csoonline.com/article/3648592/outdated-iot-healthcare-devices-pose-major-security-threats.html

49. West JB. The physiological challenges of the 1952 Copenhagen poliomyelitis epidemic and a renaissance in clinical respiratory physiology. J Appl Physiol. 2005 Aug;99(2):424–32.

50. Awad A, Trenfield SJ, Pollard TD, Ong JJ, Elbadawi M, McCoubrey LE, et al. Connected healthcare: Improving patient care using digital health technologies. Advanced Drug Delivery Reviews. 2021 Nov 1;178:113958.

51. Mitchell M, Kan L. Digital Technology and the Future of Health Systems. Health Systems & Reform. 2019 Apr 3;5(2):113–20.

52. Woods B, Coravos A, Corman JD. The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint. Journal of Medical Internet Research. 2019 Mar 19;21(3):e12568.

53. Carmody S, Coravos A, Fahs G, Hatch A, Medina J, Woods B, et al. Building resilient medical technology supply chains with a software bill of materials. npj Digit Med. 2021 Feb 23;4(1):1–6.

54. Tully J, Jarrett M, Savage S, Corman J, Dameff C. Digital Defenses for Hacked Hearts: Why Software Patching Can Save Lives. Journal of the American College of Cardiology. 2018;72(1):126–7.

55. NHS England. Clinical guidelines for major incidents and mass casualty events. Accessed May 2023. Available from: https://www.england.nhs.uk/publication/clinical-guidelines-for-major-incidents-and-mass-casualty-events/

Supplementary Files

Multimedia Appendixes

The COREQ (COnsolidated criteria for REporting Qualitative research) Checklist.
URL: http://asset.jmir.pub/assets/be465ab1df3b4e5130b41c8b41b32eb4.pdf

Supplementary Material: Workshop Scenarios for Dealing with Connected, Intelligent Medical Device Vulnerabilities and Failures.
URL: http://asset.jmir.pub/assets/c273a7a6b122fd4677cc34caac1c79e1.docx