Dresden University of Technology

Medical Device Regulatory Science
Else Kröner Fresenius Center for Digital Health

'Status quo' AI Regulation: Frameworks and Implications for Healthcare:

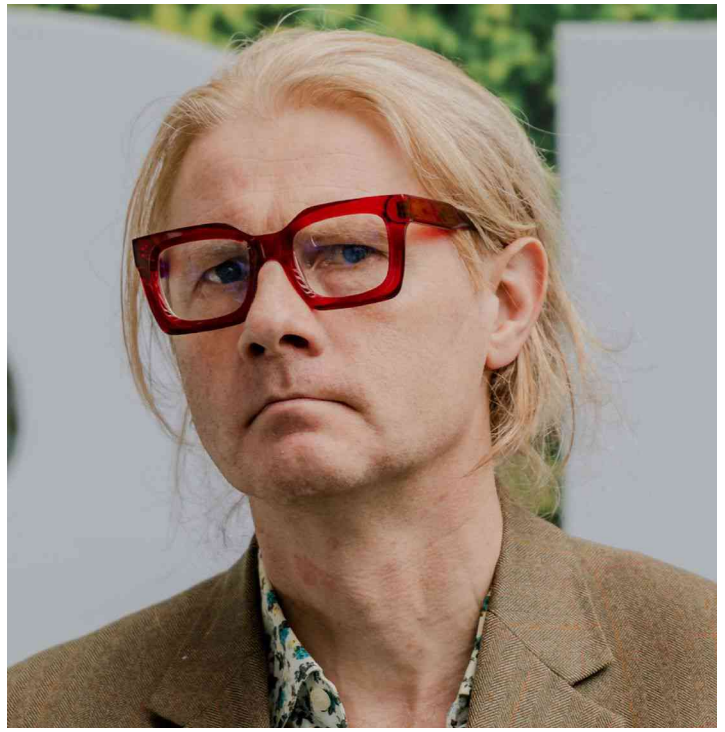
Focus 'device thinking' and focus 'Europe'

14/11/2025

Disclosures (3 years)

COMPANIES:
- Ada Health GmbH (ongoing)
- Flo Ltd (ongoing)
- haleon plc (2025 – 2026)
- AMBOSS SE (2026)

GOVERNMENT
- Expert Advisor: European Commission Directorate General Research & Innovation and SANTE (2025)
- Expert Advisor: Saudi Arabia FDA (2025 & 2026)



Prof. Dr. Stephen Gilbert
Professor of Medical Device Regulatory Science, Else Kröner Fresenius Center for Digital Health, Faculty of Medicine Carl Gustav Carus, TUD Dresden University of Technology

Faculty of Business and Economics, TUD Dresden

10:45 - 12:15 (90 mins)

10:45 - 11:25:	Regulation of medical devices
11:25 - 11:30	Questions: regulation of medical devices
11:30-12:10	Regulation of LLMs, GenAI, Agents
12:10-12:15	Questions: regulation of LLMs, GenAI, Agents

Professor, researcher, key opinion leader - medical device / IVD regulation, RegTech, AI in medicine regs

Prof. Dr. Stephen Gilbert, Professor of Medical Device Regulatory Science

Manager - Clinical Evaluation
BIOTRONIK, Berlin

2017

2019

Director Clinical Evaluation and Clinical Studies, Ada Health GmbH, Berlin

Oversaw entire clinical evaluation process, closely integrated with vigilance and PMS

2022

Professor of Medical Device Regulatory Science, TU-Dresden

First full professor in this field in Germany, one of the first in the EU

2024

Course Director: MBA Healthcare AI transformation
Expert Advisor: European Commission Directorate General Research & Innovation and SANTE and Saudi Arabia FDA (alongside professor role)

Government Projects: Addressing barriers to innovation, review of new regulatory initiatives, training

Why regulatory science one of the biggest questions of this decade and the next?

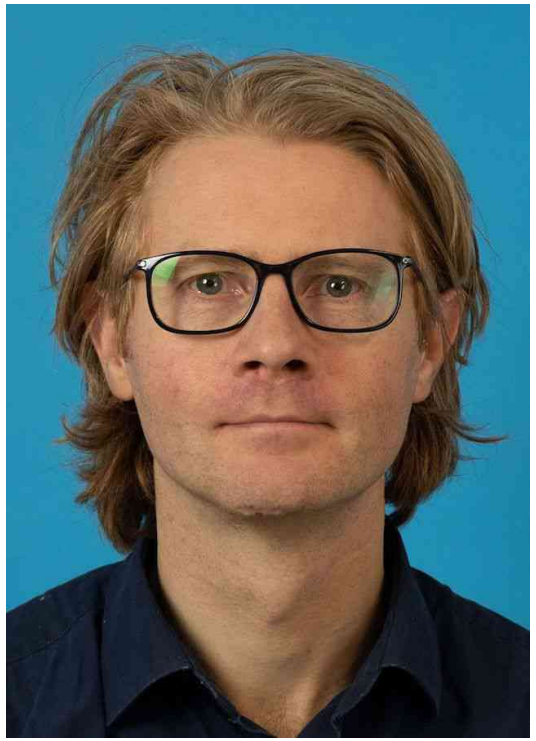
"[the EU is caught in a middle technology trap … over / over complex regulation is a large part of the problem and this is an existential threat to the future of EU competitiveness]"

- Expert research projects and lead author on working papers with the EU commission [Forthcoming 2025]

The societal role of the AI regulatory scientist …

“The antichrist comes to power by talking constantly about Armageddon, about rumours of wars and scaring you into giving him control over science and technology,"

Peter Thiel, 2025 (owner of / investor in of some of the world’s biggest technology companies)



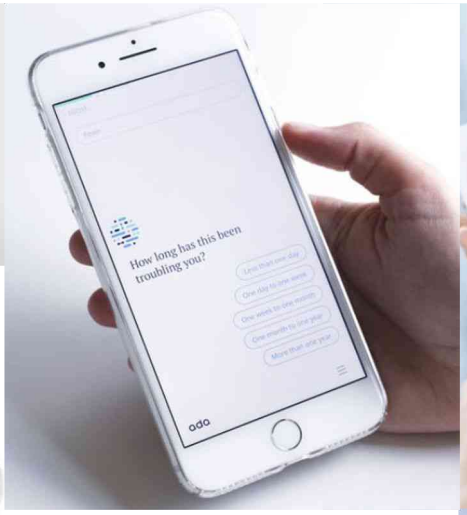
Themes

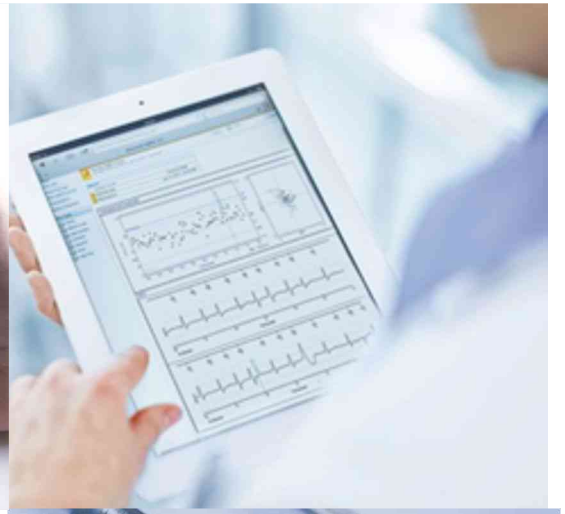
1. What is a ‘medical device’?
2. Why are medical devices regulated?
3. How are medical devices regulated?
4. Why regulate AI at all?
5. Why regulate AI as a ‘medical device’?
6. How is AI regulated as a device in the EU?
7. Some challenges with regulating AI as a ‘device’
8. Some new approaches in regulation
9. Some even bigger in regulating newer AI as a ‘device’
10. Some differences between US and EU regulation of AI – and who is ‘right’?
11. Some interesting US approaches

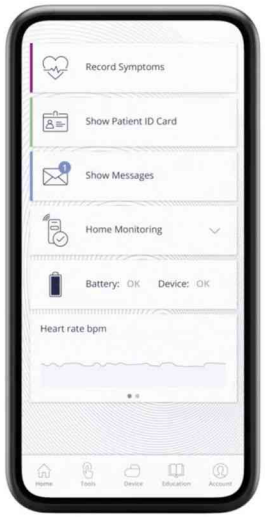
Dresden University of Technology

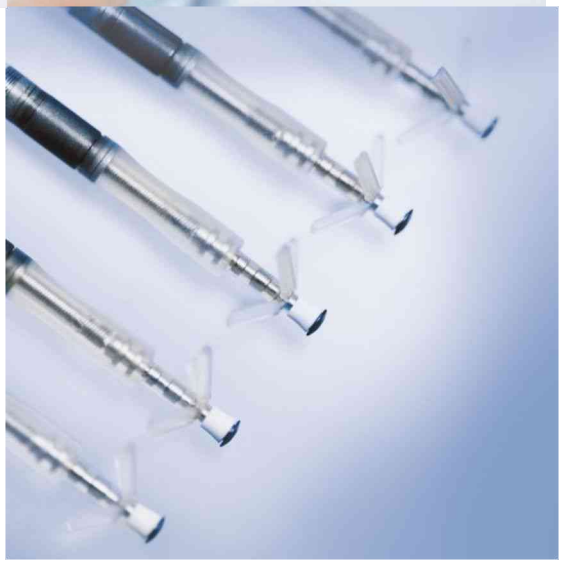
What is a medical device?

What is a medical device?

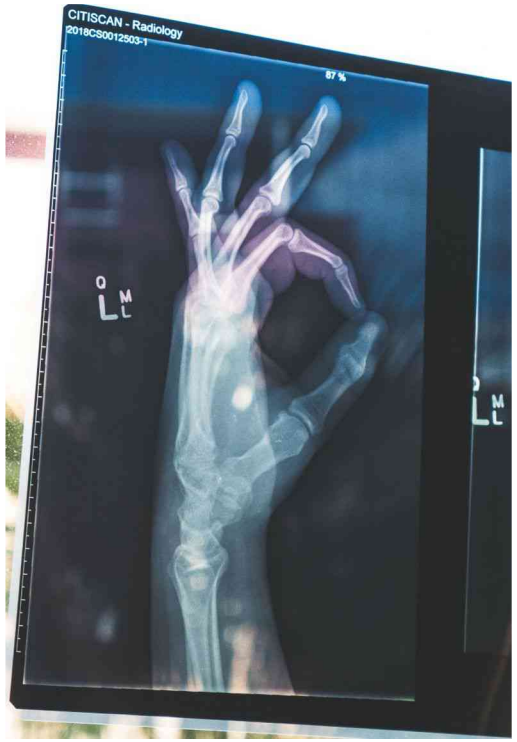






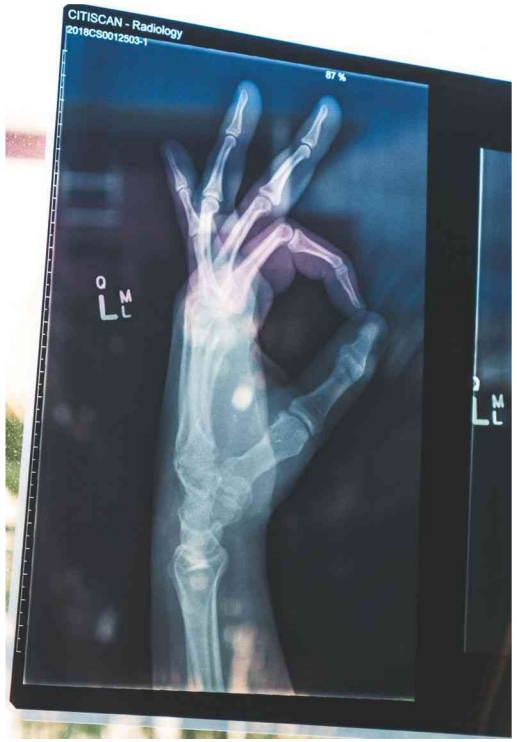


What is a medical device?
…a thing intended for:



- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease / compensation for injury
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- information by means of in vitro examination of specimens

What is an IVD? …a thing…

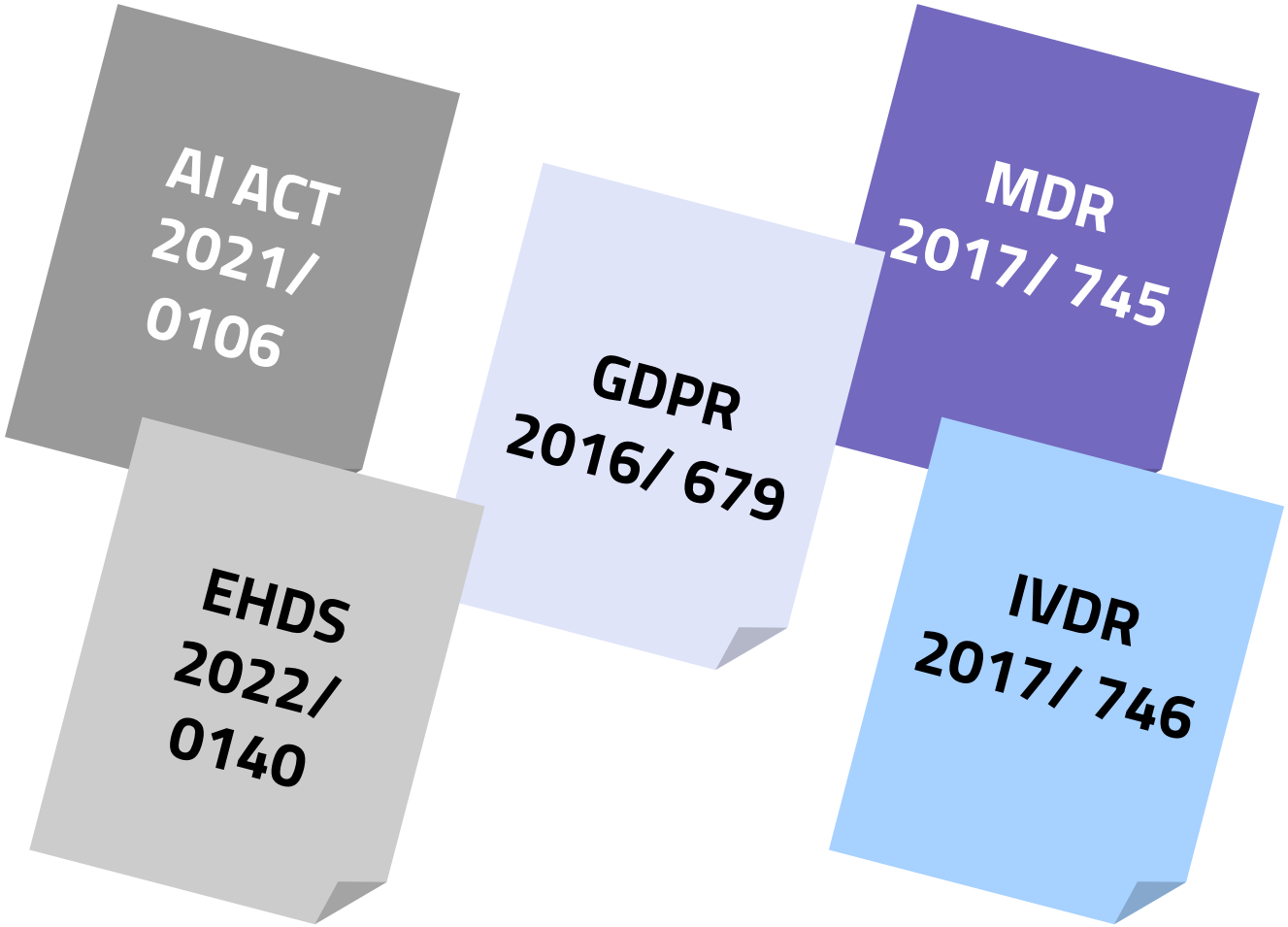


- including - any medical device which is a reagent, reagent product, calibrator, control material, kit, instrument, apparatus, piece of equipment, software or system
- **intended by the manufacturer** to be used in vitro for the examination of specimens, including blood and tissue donations, derived from the human body, solely or principally for the purpose of providing information … **by means of in vitro examination of specimens**

Dresden University of Technology

What is the status quo regulation of medical devices?

Medical Device Regulatory Science



Prof. Dr. Stephen Gilbert

Professor of Medical Device Regulatory Science

Else Kröner Fresenius Center for Digital Health

TUD Dresden University of Technology

What is (the) medical device regulation?

" …aims to **ensure the smooth functioning of the internal market as regards medical devices**, taking as a base a high level of protection of health for patients and users, and taking into account the small- and medium-sized enterprises that are active in this sector. …objectives …not being secondary to the other."

5.5.2017 EN Official Journal of the European Union L 117/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 5 April 2017

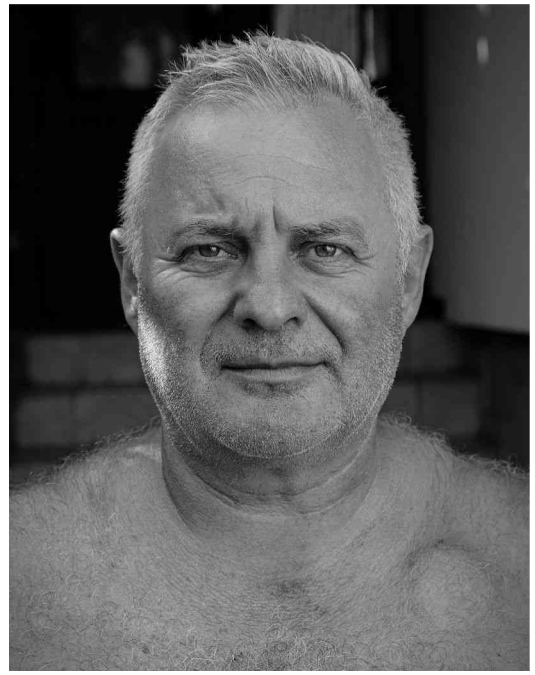
on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

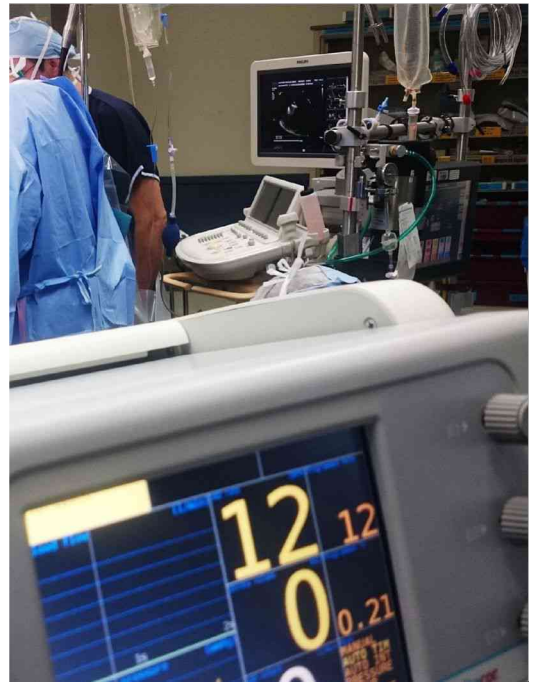
What is (the) medical device regulation?

- Approval Process and Restrictions on Placing on Market
- Systems and Special Device Cases
- Oversight of Claims
- Obligations, Specifications, Standards and Definitions
- Identification and Conformity Assessment
- Intended Purpose, Intended Use



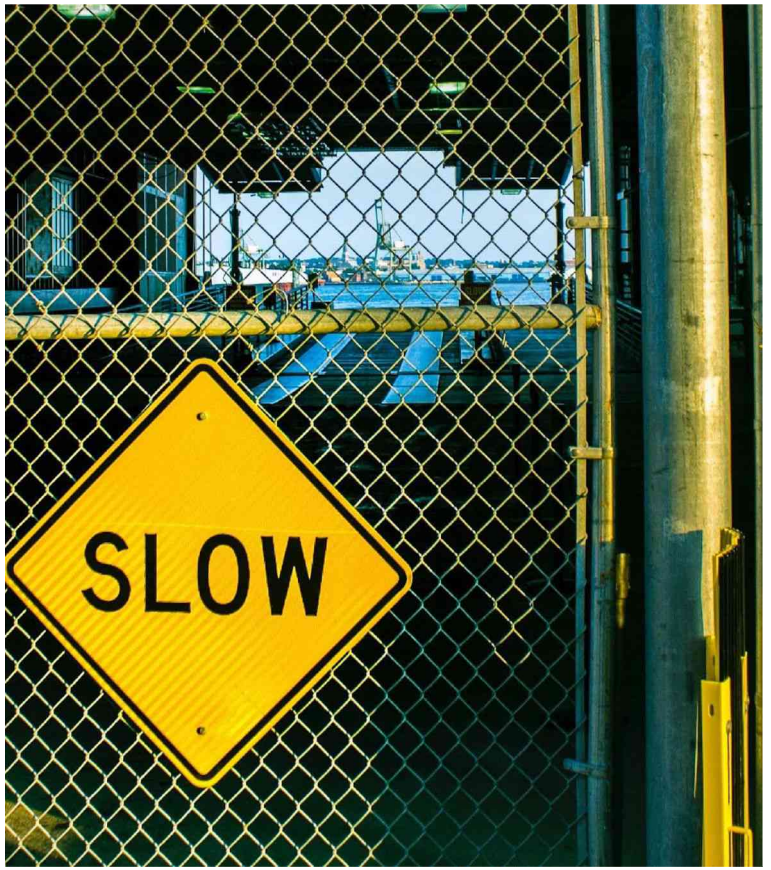
What is (the) medical device regulation?

- Quality Management (QMS)
- Qualification, Classification, Risk Class
- Clinical Evaluation
- Usability, Engineering, Human Factors
- Risk Assessment
- Clinical Investigation and Post Market Surveillance (PMS)



‘regulatory AFFAIRS’

- ”MDR says x – you must …”
- “Have you done …?”
- “Have you followed ISO######:#####…?”
- “Is your evidence for performance of the device good enough to show ….?”
- “I will not sign document x until you do y.”



‘regulatory SCIENCE’

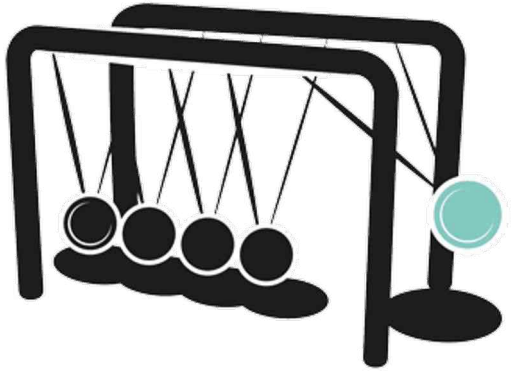
- What is the evidence this regulation produces better outcomes…?
- What alternative ways of regulating are there…?
- What are the unintended outcomes…?
- What regulatory approach is needed for new technology x…?
- Can this regulation be delivered safety but automated, faster?

Dresden University of Technology

Why do we need medical device regulation?: Was MDR/IVDR necessary?

The problem...

The problem.... Is regulation necessary?



"I don't want to have a ticking time bomb inside me"

– PIP breast implant recipient

ICIJ INTERNATIONAL CONSORTIUM of INVESTIGATIVE JOURNALISTS

DePuy metal-on-metal hip implants

- agreed to pay $4 billion
- 8000 lawsuits

The problem …. Is regulation necessary?

Update: Certain [redacted] Ventilators, BiPAP Machines, and CPAP Machines Recalled Due to Potential Health Risks: FDA Safety Communication

Since April 2021 through April 30, 2022, the FDA received more than 21,000 MDRs, including 124 reports of death, associated with the PE-PUR foam breakdown or suspected foam breakdown. The MDRs received included both mandatory reports from [redacted] and voluntary reports from health professionals, consumers, and patients. A wide range of injuries have been reported in these MDRs, including cancer, pneumonia, asthma, other respiratory problems, infection, headache, cough, dyspnea (difficulty breathing), dizziness, nodules, and chest pain.

Content current as of:
05/19/2022

Regulated Product(s)
Medical Devices

The problem …. Is regulation necessary?

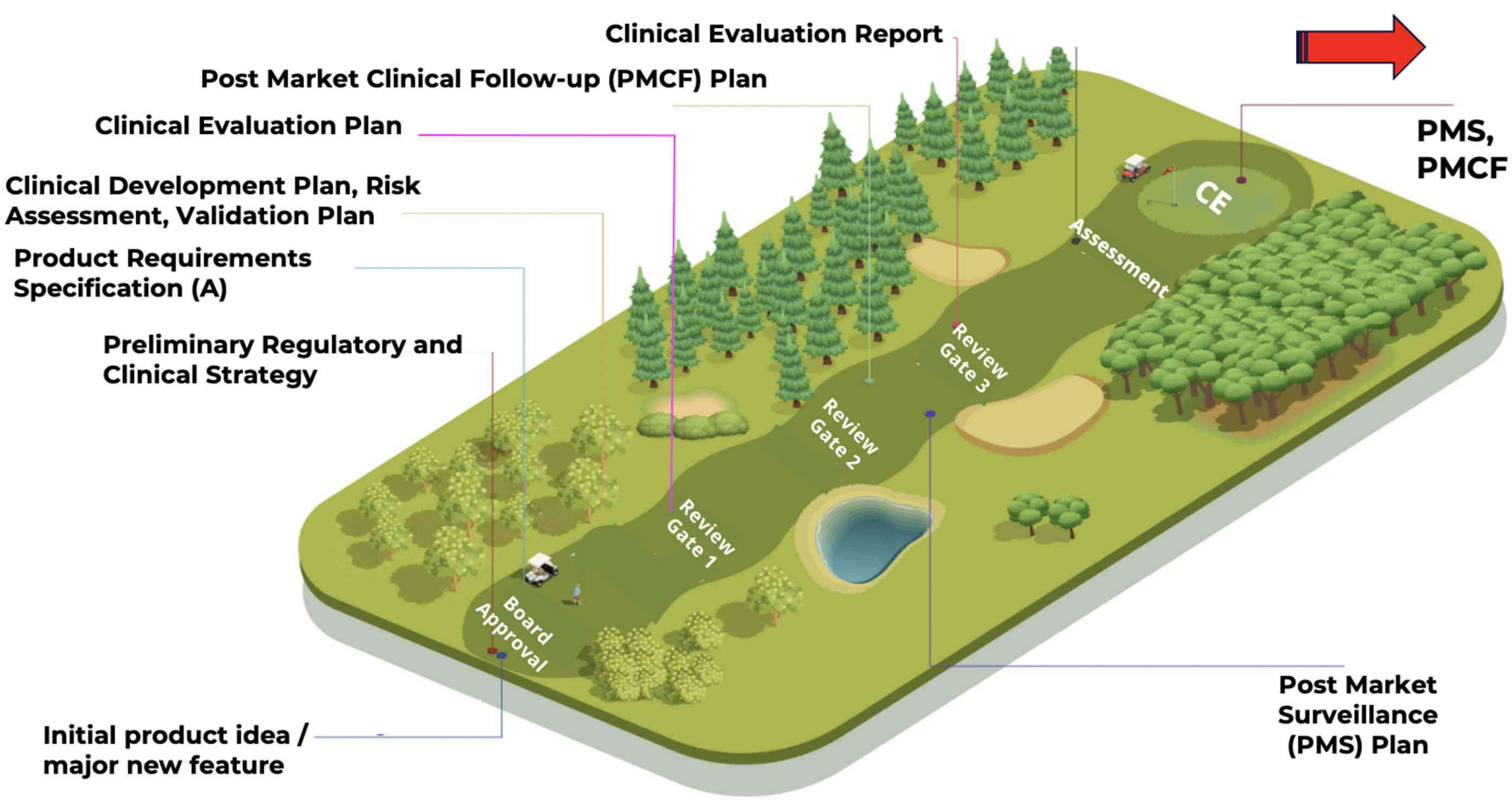
"…the [redacted] Sepsis Model has poor discrimination and calibration in predicting the onset of sepsis… raises fundamental concerns about sepsis management on a national level."

– Wong et al., 2021, JAMA Intern Med 181(8):1065-70.

Dresden University of Technology

The regulation of modern AI enabled Digital Medical 'Devices' in MDR/IVDR/AI Act?

The TPLC from tee to green (focus clinical) …



- pivot
- design thinking
- design iteration
- continuous release
- grouping of DMDs in suites
- DMD embedded/co-designed in workflows

The challenge… DMDs are/will be

Systems

Modular

Agile

Design Thinking

Learning from Data

Move Fast

Is your conception of AI fixed?

IG·NB
Interessengemeinschaft der Benannten Stellen für Medizinprodukte in Deutschland

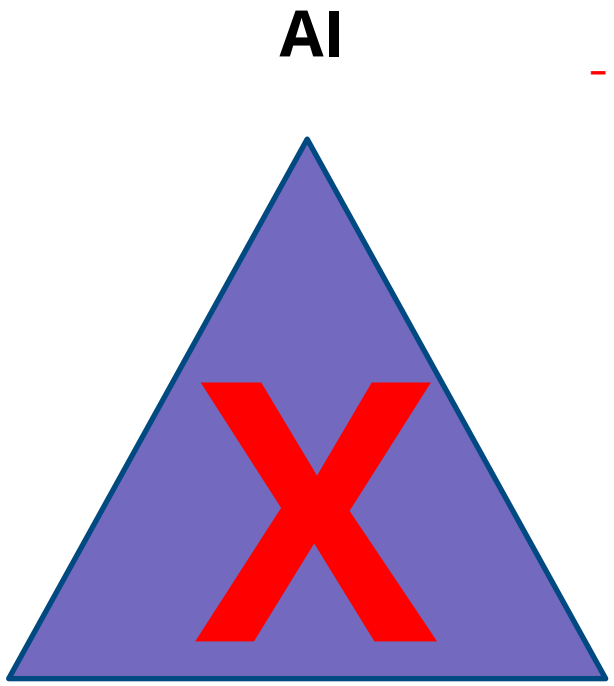
A) General requirements

1. Certifiability of AI

Static AI (AI that has learned and operates in a learned state) is in principle certifiable.

Dynamic AI (AI that continues to learn in the field) is not certifiable in principle, as the system must be verified and validated (among other things, the functionality must be validated against the intended use).

The challenge …



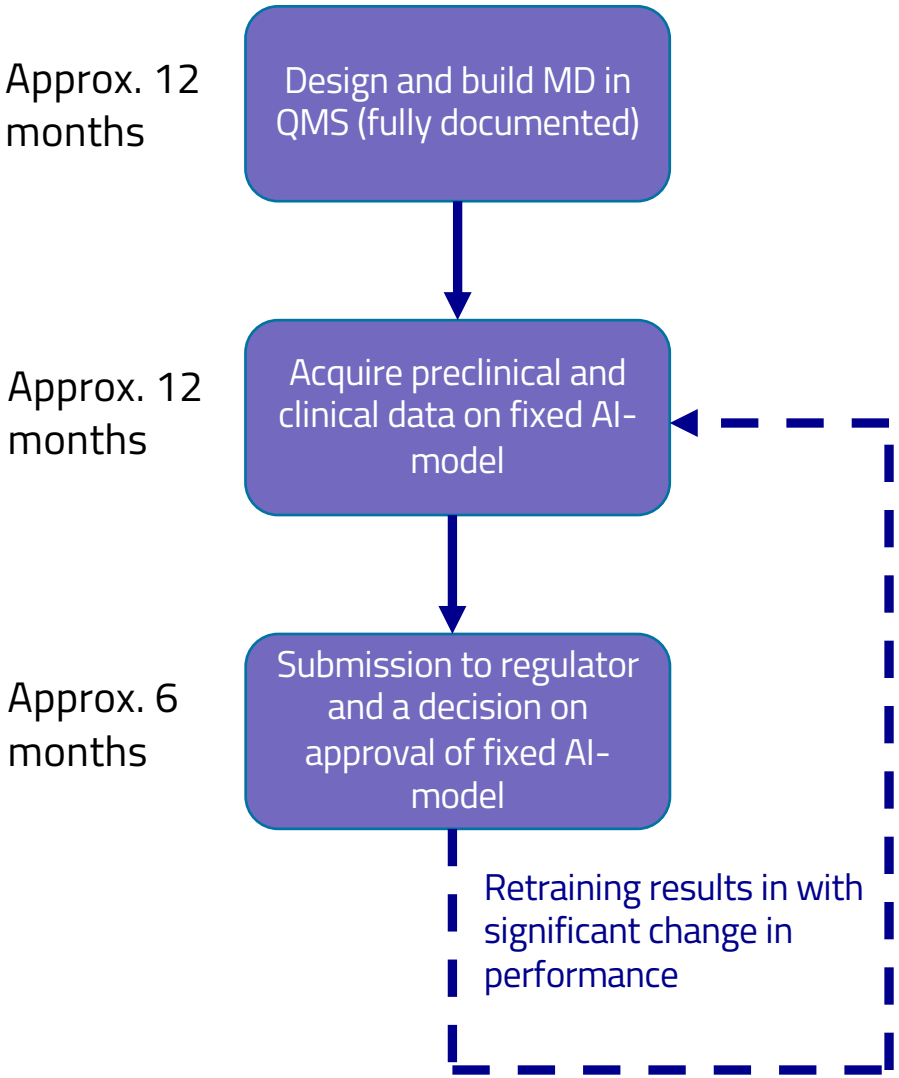
- everything be documented
- all change must be pre-approved

digitization /
digital health

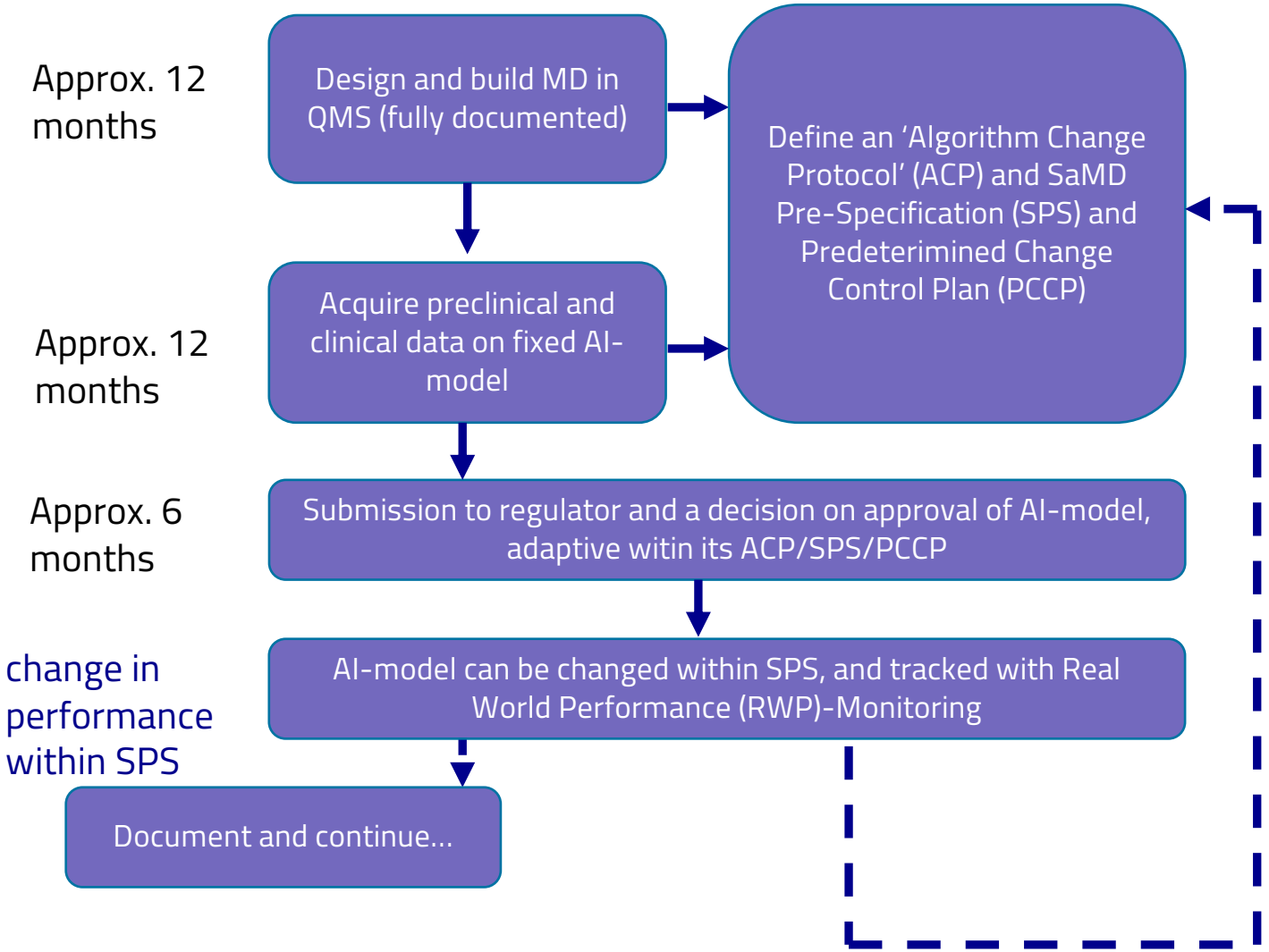
biomedical
engineering /
biotechnology

change
adaption
flexibility
personalisation
digital twins

ACP/PCCP/SPS: ‘old’ model



ACP/PCCP/SPS: proposed model (US FDA ..)

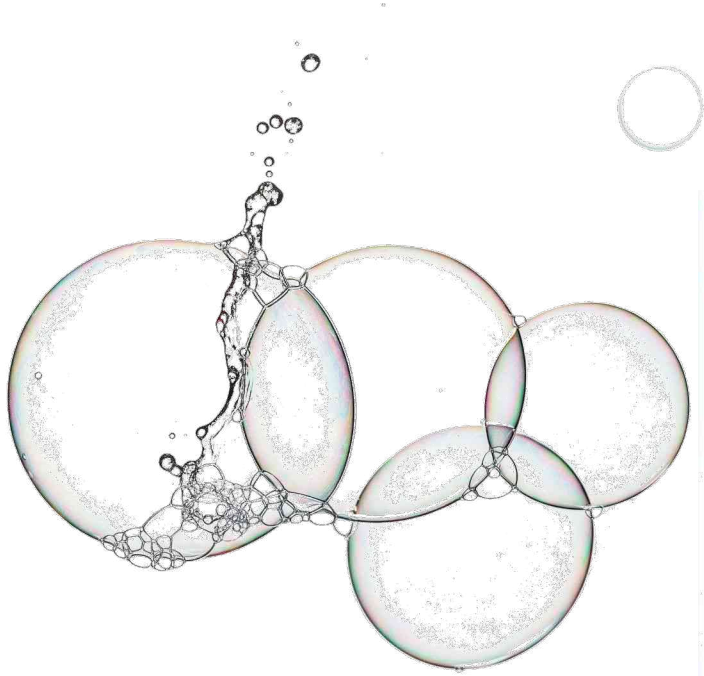


Dresden University of Technology

(22.5 mins): And then it became even harder …. Large Language Models in Medicine

- … not all bad …
- … and not all good …
- … and definitely not to be ignored!

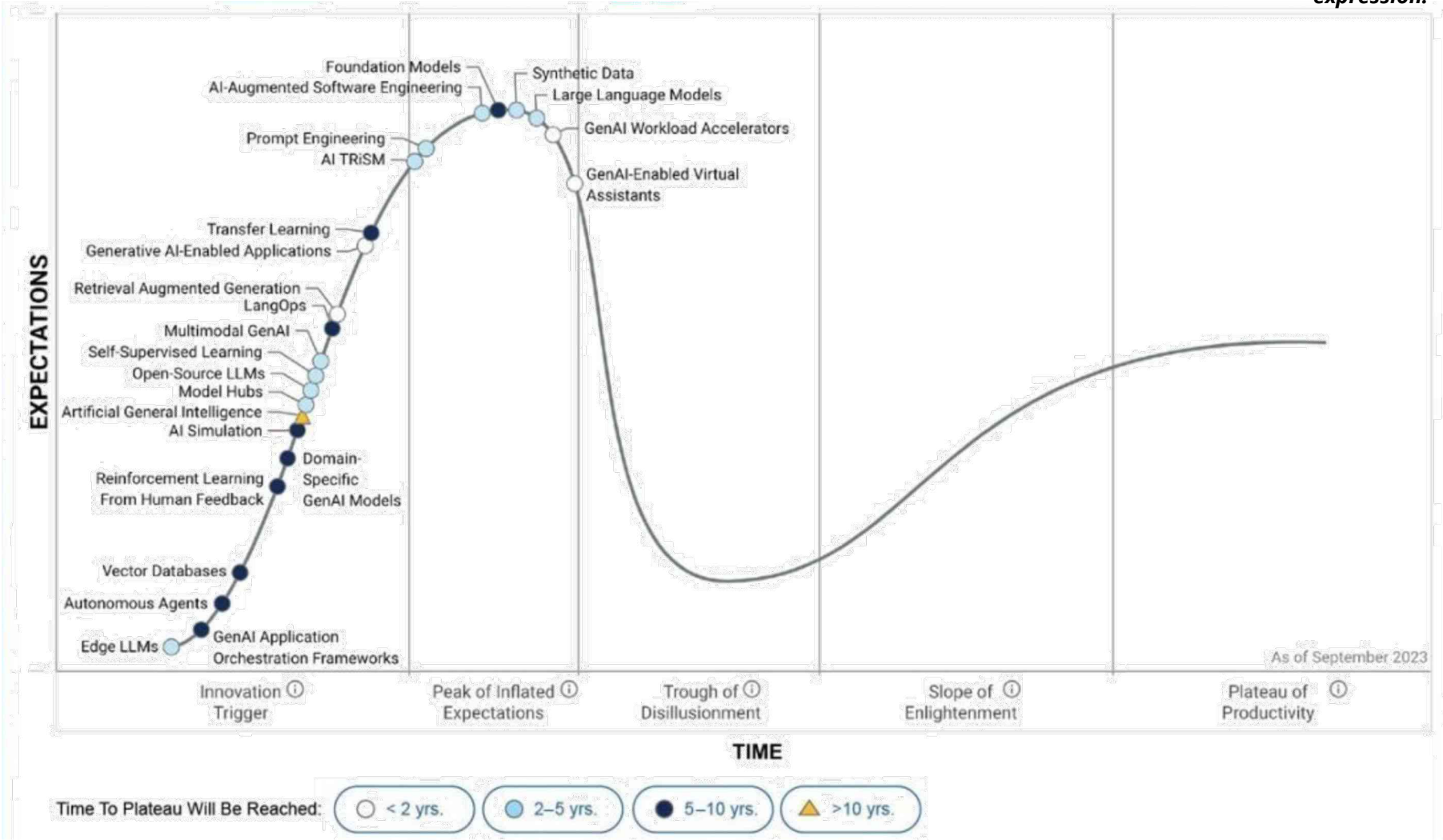
1. The hype / bubble …



Gartner

Gartner
2,051,838 followers
7mo •

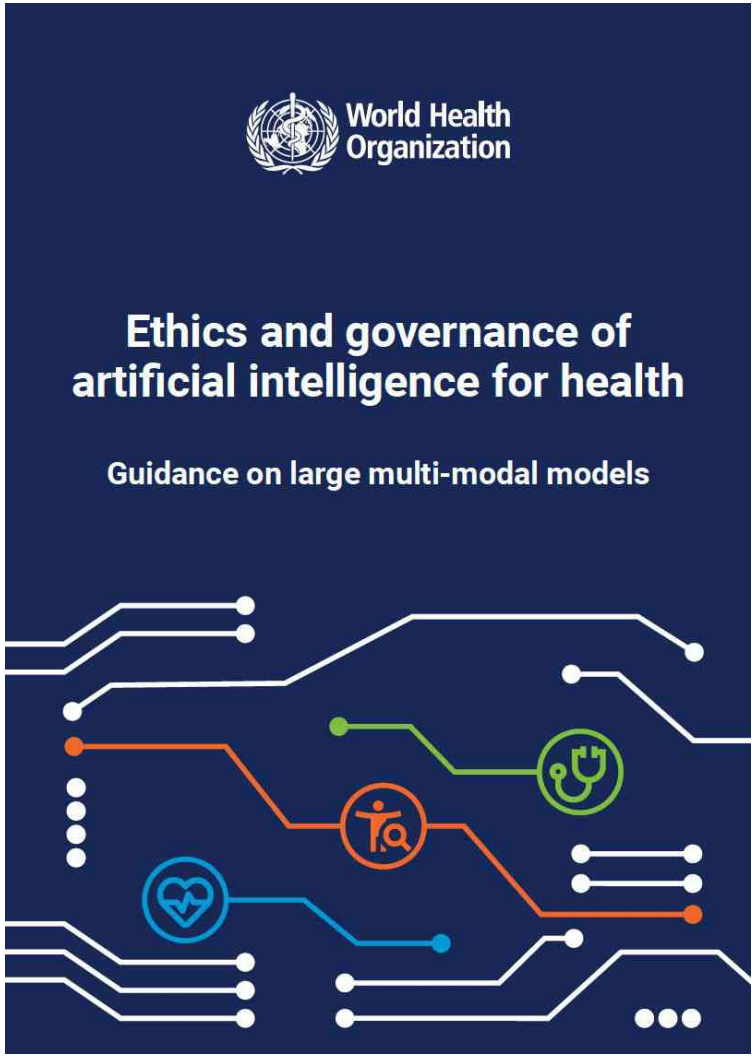
Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.



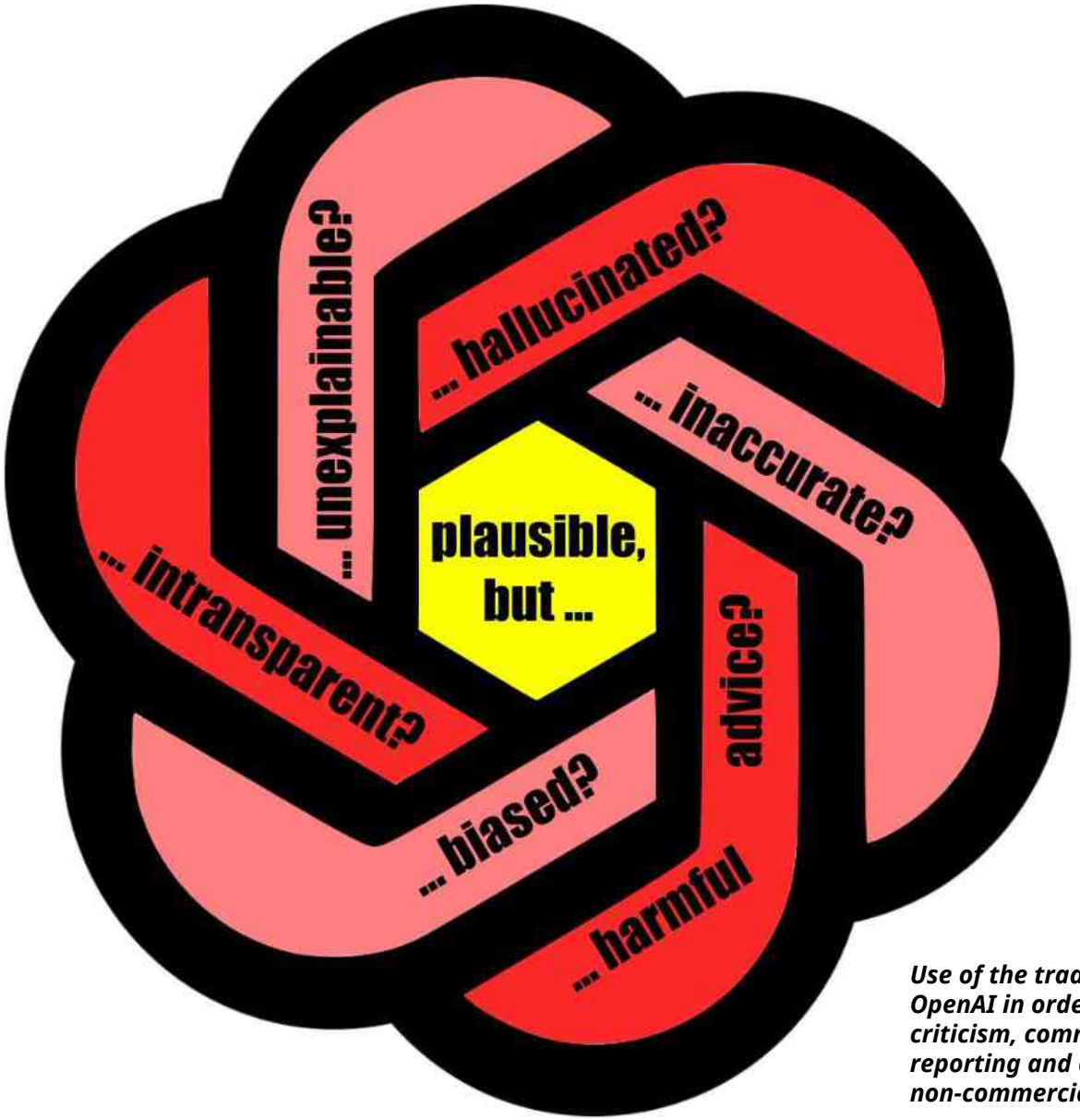
2. Technology with promise (in LMICs) …

Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.

World Health Organisation
Meet Sie S.A.R.A.H.
a Smart AI Resource Assistant for Health
She uses generative AI to help you live a healthier life



3. Technology with inherent weaknesses …



nature medicine

Search Log in

Content About Publish

comment > article

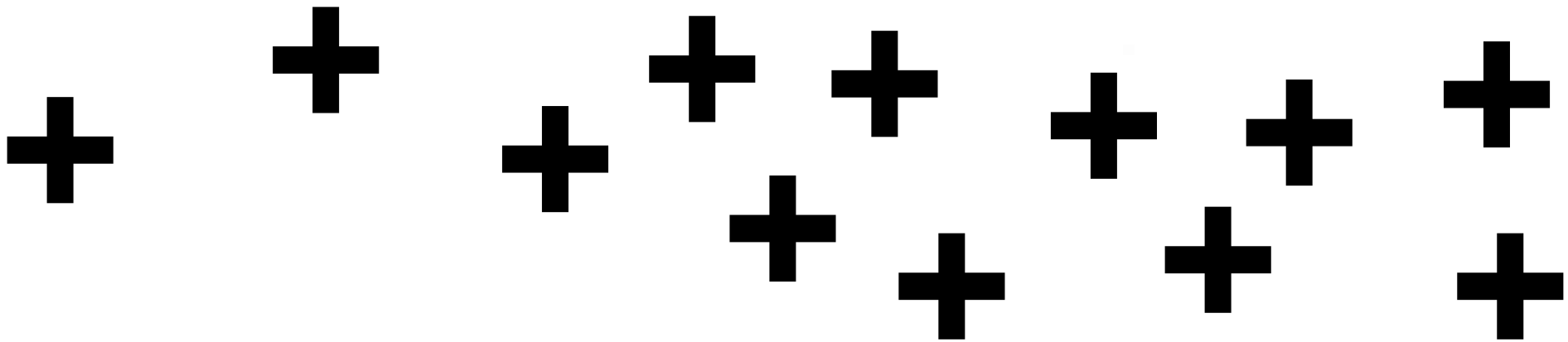
Comment | Published: 30 June 2023

Large language model AI chatbots require approval as medical devices

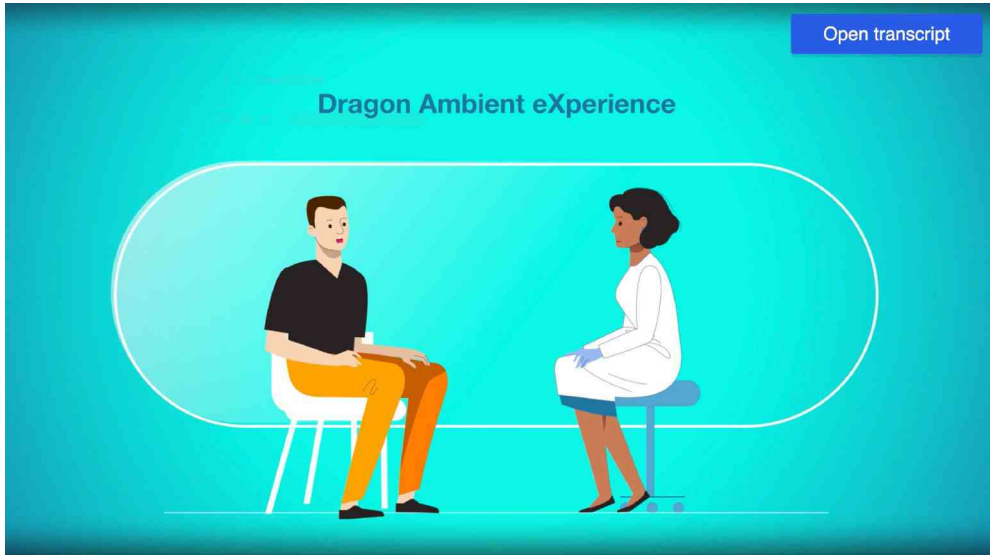
Stephen Gilbert, Hugh Harvey, Tom Melvin, Erik Vollebregt & Paul Wicks — Show fewer authors

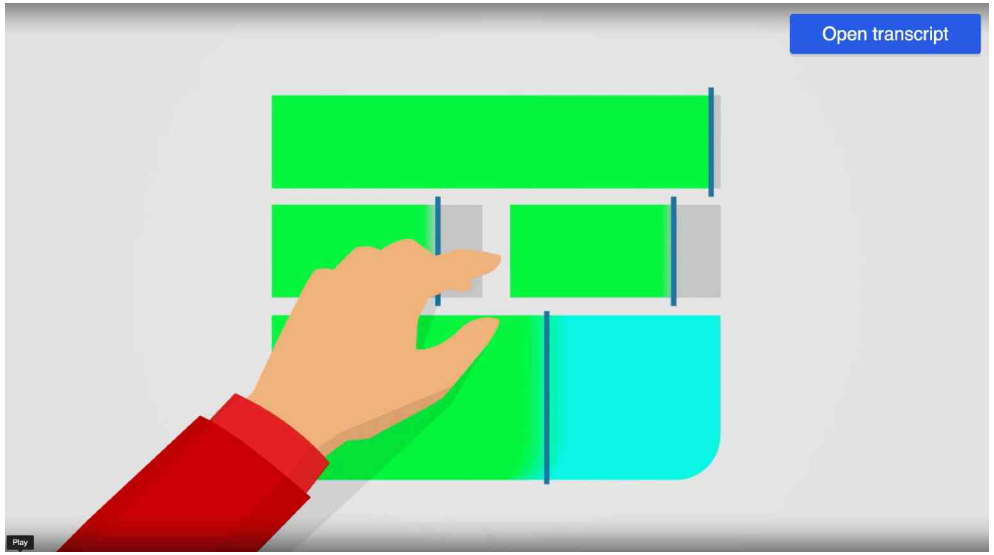
4. Technology with high pervasiveness ...

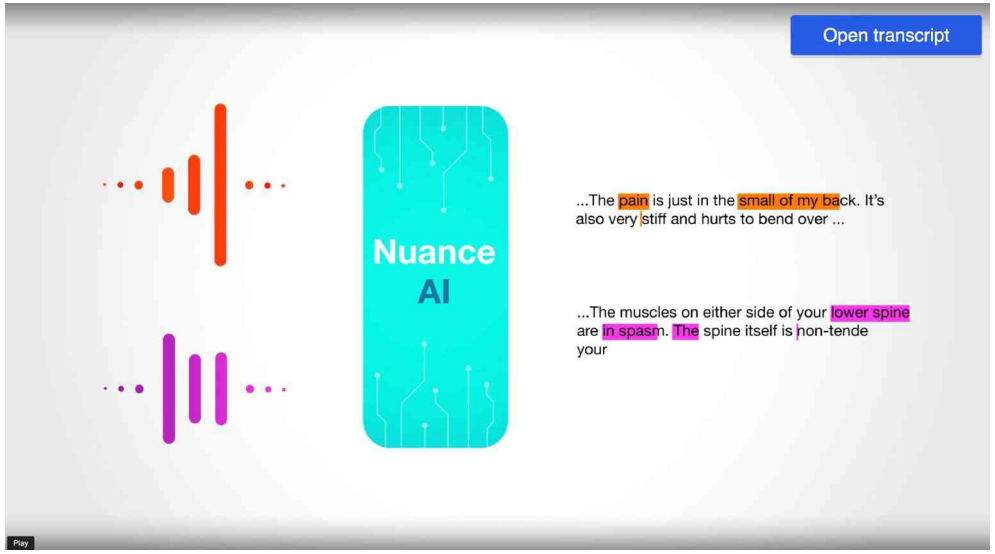
Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.

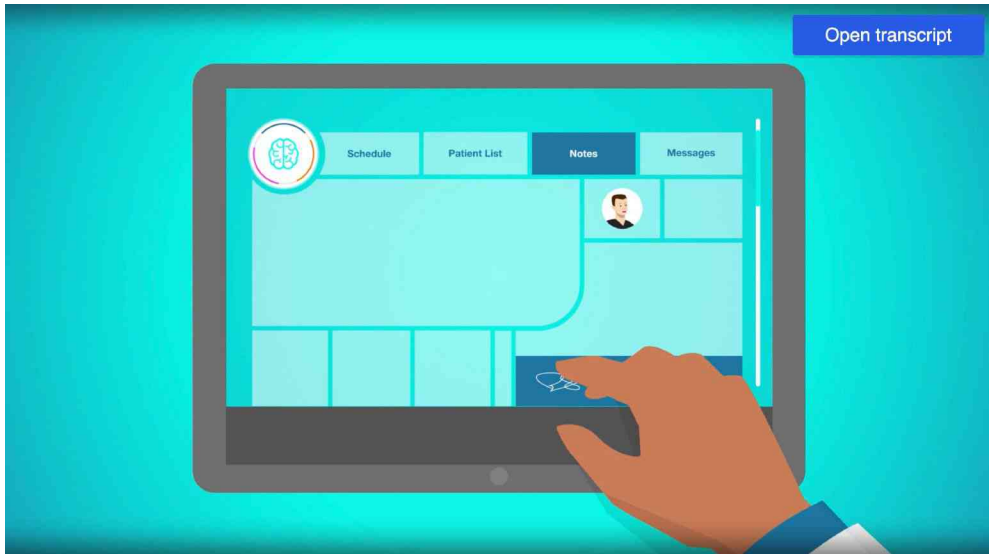


5. Technology with early ‘killer’ use cases …





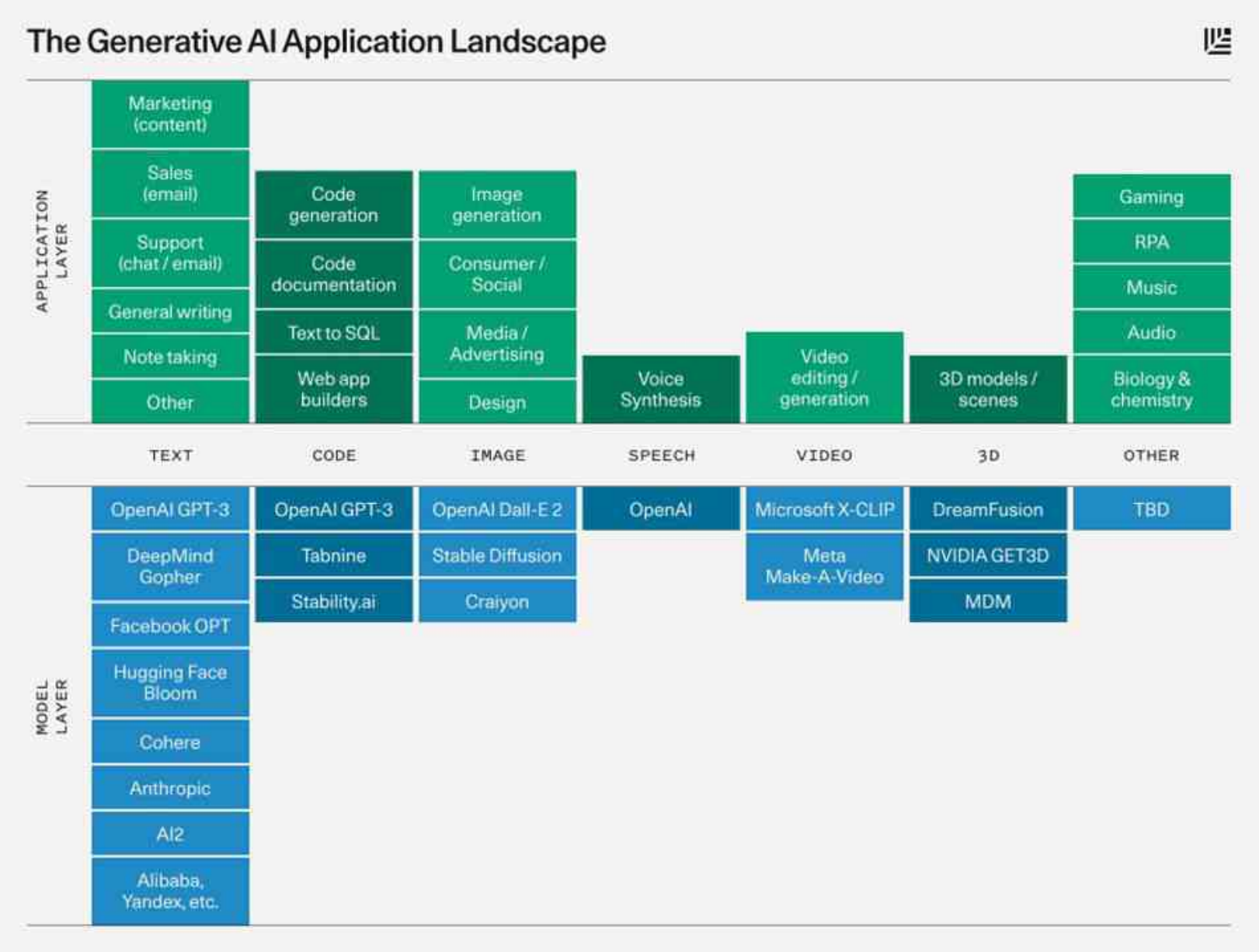




Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.

NUANCE

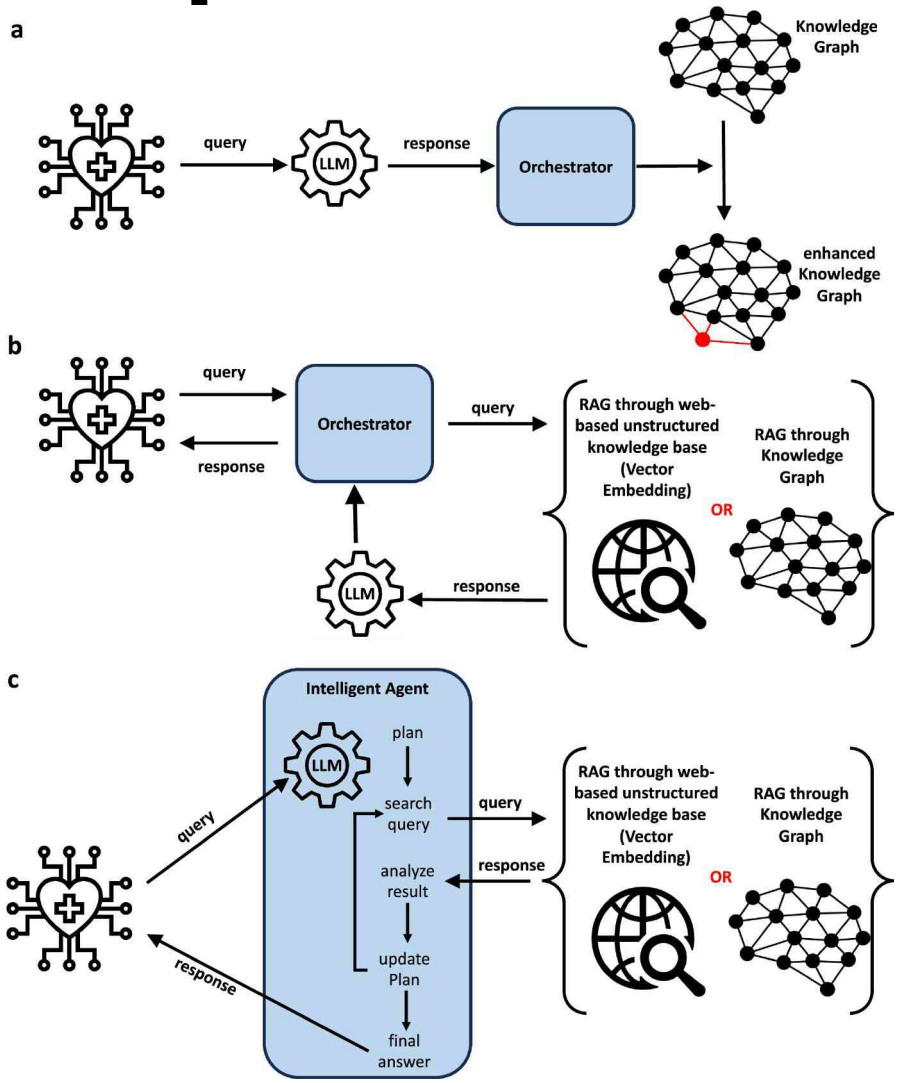
6. Technology with multimodality …



Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.

Source: 'The Power of Generative AI: Exploring its Impact, Applications, Limitations, and Future' Jacques Ludik

7. Technology that is augmentable / shape shifter…



npj | digital medicine

Explore content · About the journal · Publish with us

nature › npj digital medicine › news & views › article

News & Views | Open access | Published: 23 April 2024

Augmented non-hallucinating large language models as medical information curators

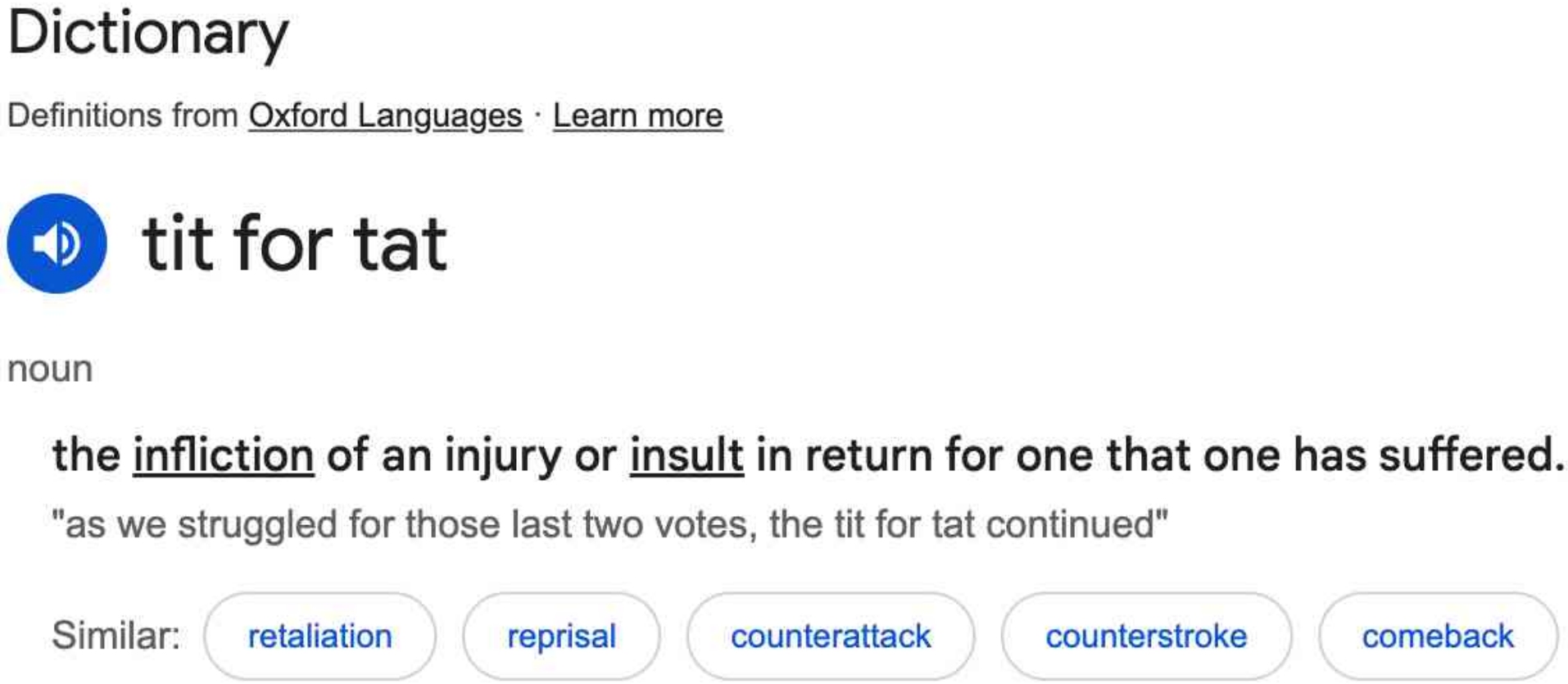
Stephen Gilbert, Jakob Nikolas Kather & Aidan Hogan

npj Digital Medicine **7**, Article number: 100 (2024) | Cite this article

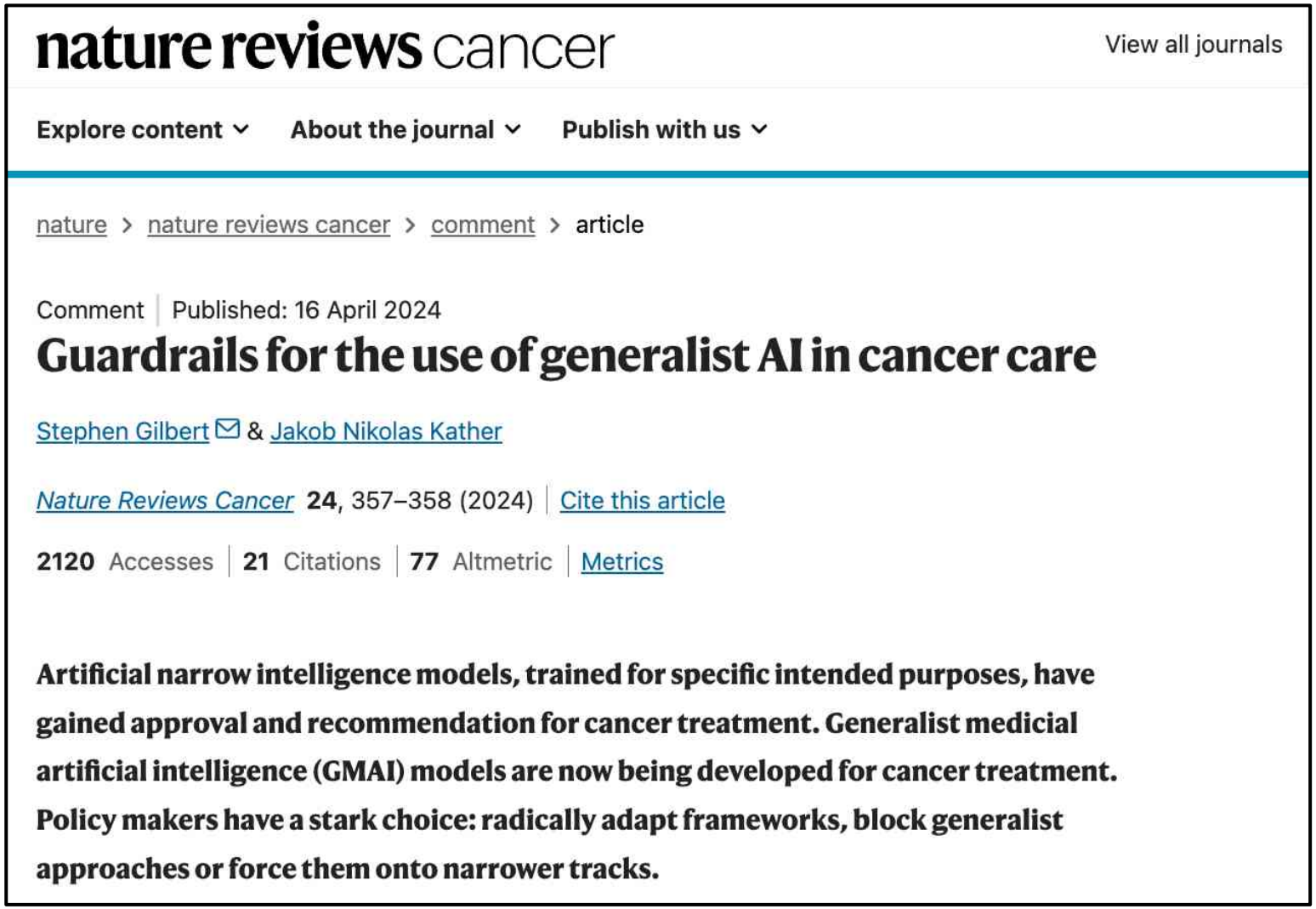
322 Accesses | **10** Altmetric | Metrics

8. ‘Scientific’ progress that is tit for tat …

Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.



9. Not like other AI or devices … broad and increasingly ‘AGI’ ‘simulant’



nature reviews cancer

View all journals

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature › nature reviews cancer › comment › article

Comment | Published: 16 April 2024

Guardrails for the use of generalist AI in cancer care

Stephen Gilbert ✉ & Jakob Nikolas Kather

Nature Reviews Cancer **24**, 357–358 (2024) | Cite this article

2120 Accesses | **21** Citations | **77** Altmetric | Metrics

Artificial narrow intelligence models, trained for specific intended purposes, have gained approval and recommendation for cancer treatment. Generalist medicial artificial intelligence (GMAI) models are now being developed for cancer treatment. Policy makers have a stark choice: radically adapt frameworks, block generalist approaches or force them onto narrower tracks.

10. An enforcement vacuum …

THE LANCET
Digital Health

This journal · Journals · Publish · Clinical · Global health · Multimedia · Events · About

VIEWPOINT · Volume 6, Issue 9, E662-E672, September 2024 · *Open Access* · Download Full Issue

A future role for health applications of large language models depends on regulators enforcing safety standards

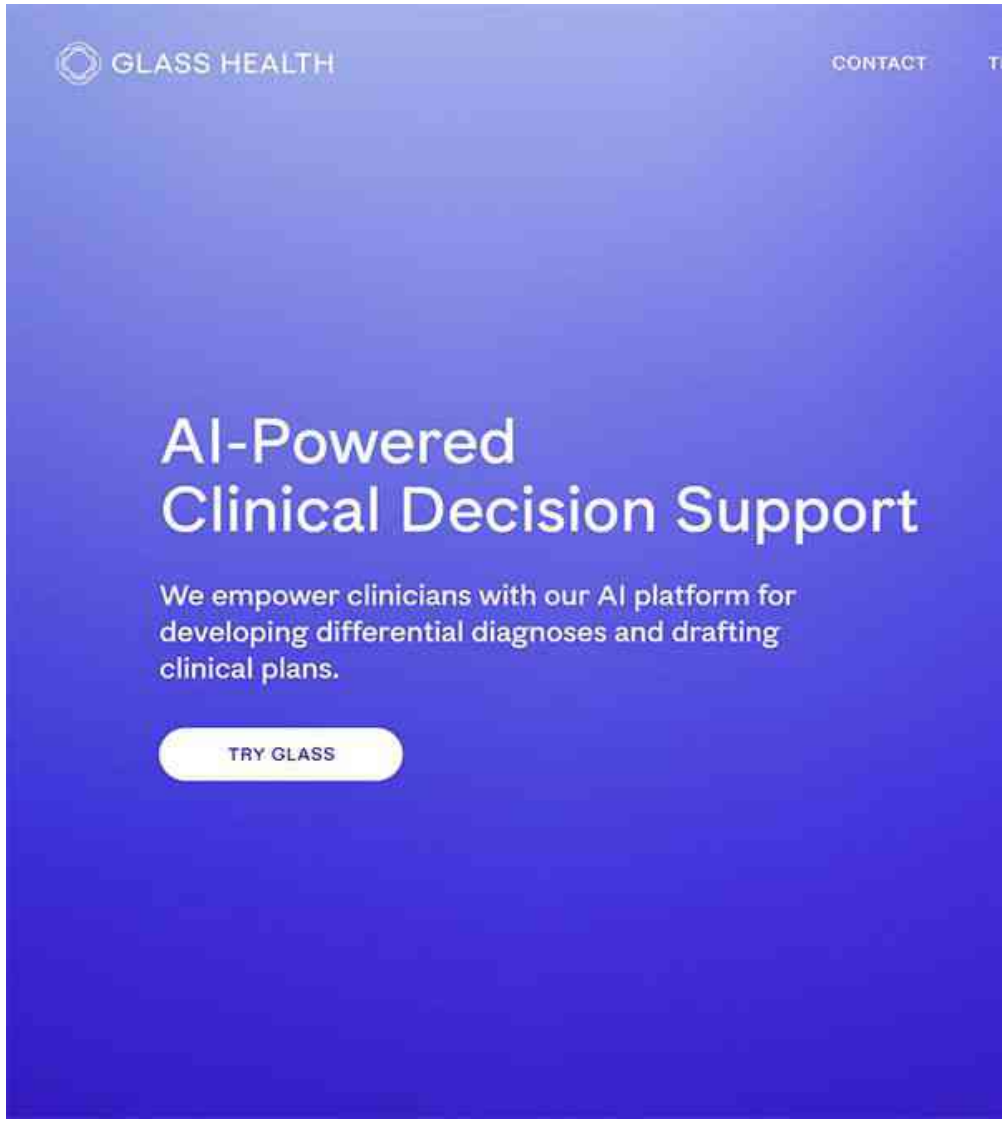
Oscar Freyer [a] · Isabella Catharina Wiest, Dr med [a,b] · Prof Jakob Nikolas Kather, Dr med [a,c,d] · Stephen Gilbert, PhD [a]

Affiliations & Notes · Article Info

	LLM-based health applications used by health-care professionals			LLM-based health applications used by laypeople		
	Rules	Medical devices on the market	Enforcement	Rules	Medical devices on the market	Enforcement
USA	Ambiguous (some might be classified as non-devices)	Yes*	Ambiguous (some might be classified as non-devices)	Ambiguous (FDA might exercise enforcement discretion† for some LLM-HAs)	Yes‡	Ambiguous (FDA might exercise enforcement discretion† for some LLM-HAs)
EU	Clear (devices for triage, diagnosis, and therapy are medical devices)	Yes*	No	Clear (devices for triage, diagnosis, and therapy are medical devices)	Yes‡	No

Figure 2: **Regulatory status and enforcement of existing rules for LLM-based health applications**
FDA=Food and Drug Administration. LLM=large language models. LLM-HA=LLM-based health applications. *Glass Health. †Some could fall under enforcement discretion.[76] ‡Health Tracker: AI Doctor.[53]

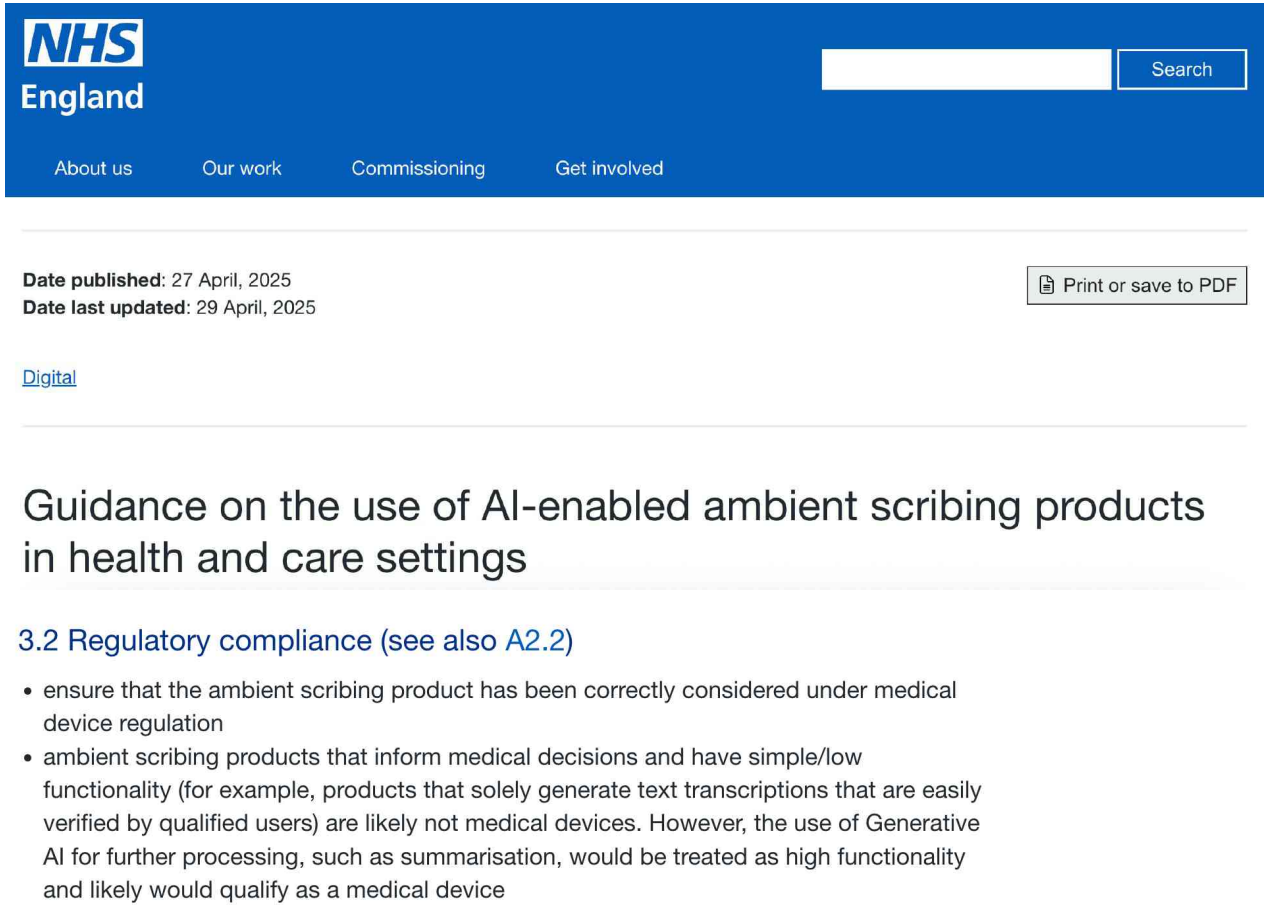
11. Unapproved on-market broad 0-shot CDS



2.4 The Services and any Company Materials made available through the Services are a **non-device** clinical decision support software application within the meaning of Section 520(o)(1)(E) of the federal Food, Drug and Cosmetic Act, 21 U.S.C. Sec. 360j(o)(1), and the **regulations and guidance issued by the U.S. Food and Drug Administration to implement that provision**. By accessing or using the Services and Company Materials, you agree to only use the Services and Company Materials in this manner and solely for this purpose. The artificial intelligence or machine learning functionality available on the Services ("Glass AI") **are intended for use only by healthcare providers** and are **not intended for use by the general public.** If you are not a healthcare provider, you are not authorized to and will not access or use the Glass AI functionality. If you access or use Glass AI, you attest that you are a healthcare provider and agree that the application is: (1) **not intended to acquire, process, or analyze a medical image or a signal** from an in vitro diagnostic device or a pattern or signal from a signal acquisition system; (2) intended for the purpose of displaying, analyzing, or printing medical information about a patient or other medical information; (3) intended for the purpose of supporting or providing recommendations to a health care professional about prevention, diagnosis, or treatment of a disease or condition; and (4) **intended for the purpose of enabling such health care professional to independently review the basis for such recommendations** that such software presents so that it is not the intent that such health care professional rely primarily on any of such recommendations to make a clinical diagnosis or treatment decision regarding an individual patient.

13. Regulatory shifting sands …

Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.



TORTUS

As a UK MHRA Class I Medical Device, TORTUS is pioneering the science of clinical safety in the AI space – the CREOLA approach we developed last year now underpins our automated clinical guardrail systems that make TORTUS the safest AVT enterprise supplier on the market. We believe AI can be powerful if deployed well, but equally can be dangerous if not, and therefore must be regulated as any drug or other medical device would be – a position that NHS England agrees with.[1]

14. Who regulates future AI …. AI / AI plc …?

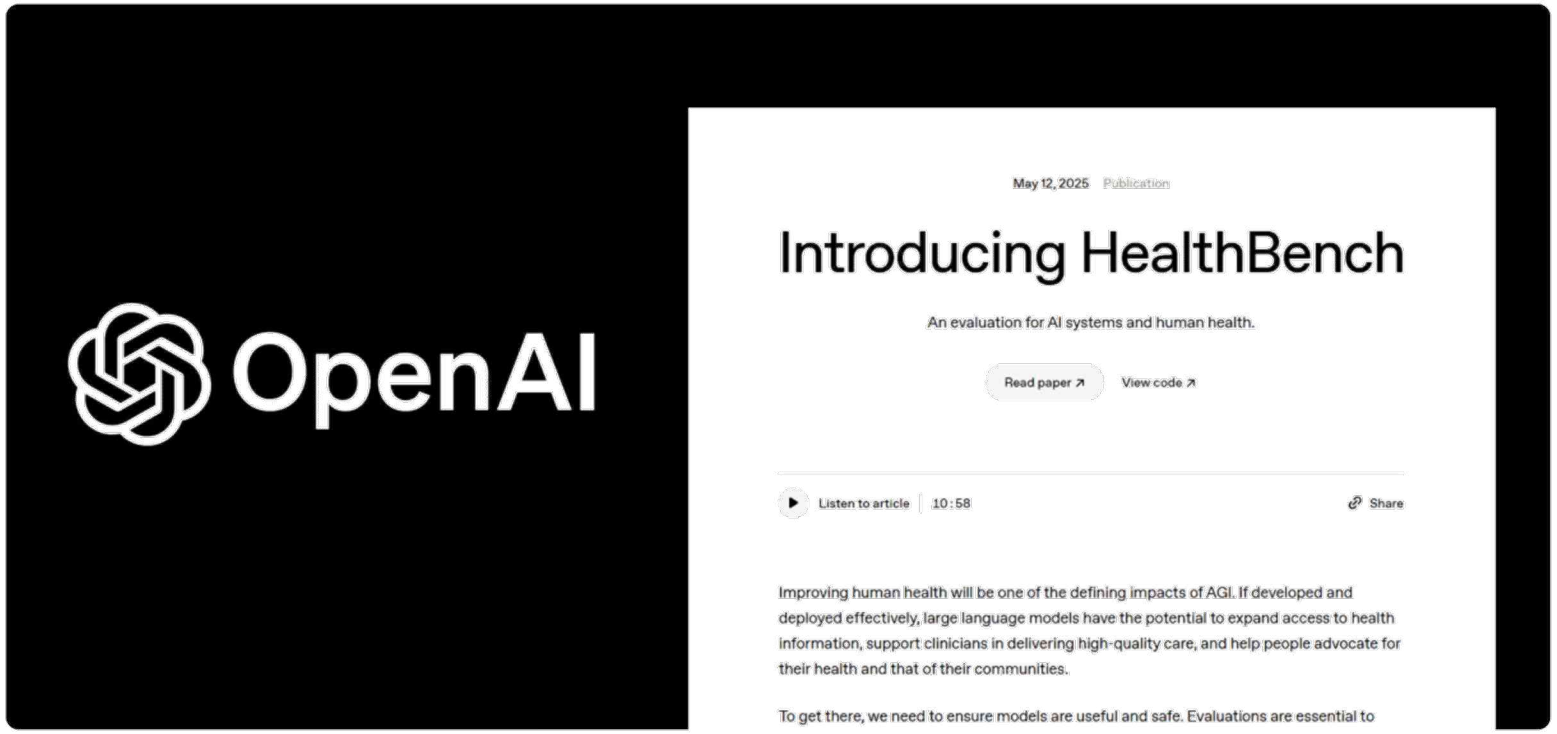
Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.

digitalhealthwire

OpenAI Dives Into Healthcare With HealthBench

MAY 15, 2025 JASON BARRY 2 MIN READ

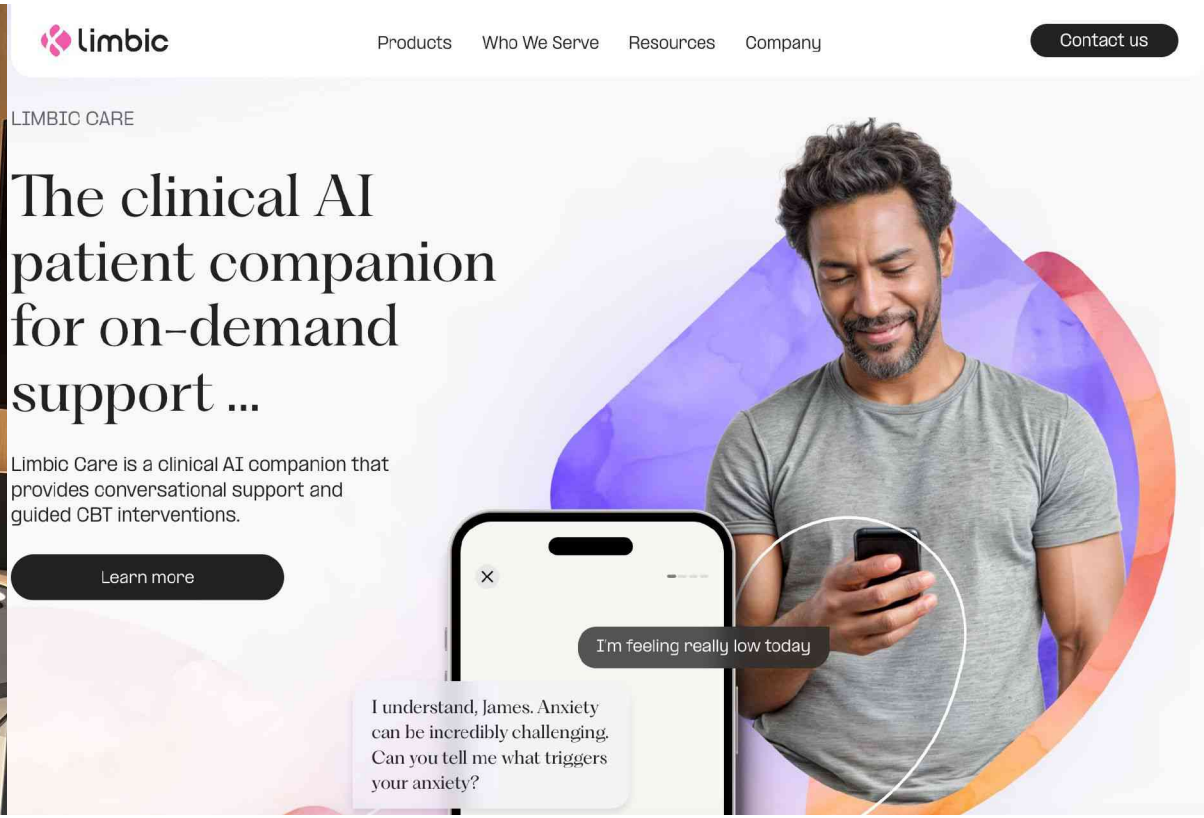
HealthBench: Evaluating Large Language Models Towards Improved Human Health Arora et al., [**PREPRINT**]
https://doi.org/10.48550/arXiv.2505.08775



“An evaluation for AI systems and human health”

12. First approvals …

Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.



CE

VALMED UNIVERSE

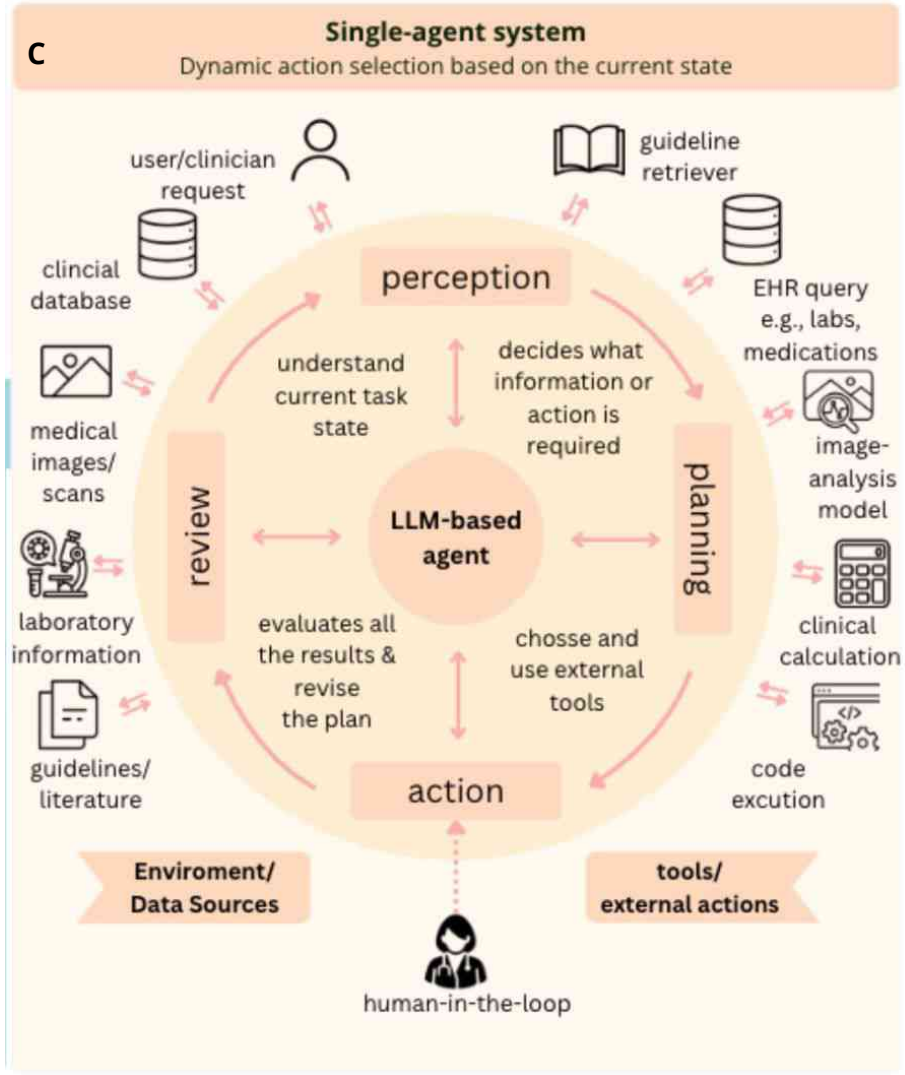
limbic

UK CA

15. The agents are coming ....

State of the art on clinical agents

**** The emerging role of agentic AI in medicine**, Narmin Ghaffari Laleh, Sanddhya Jayabalan, Oscar Freyer, Daniel Truhn, Isabella C. Wiest, Magdalena Katharina Wekenborg, Stephen Gilbert, Renato Umeton, Mamatha Bhat, Jakob Nikolas Kather [In Preparation]



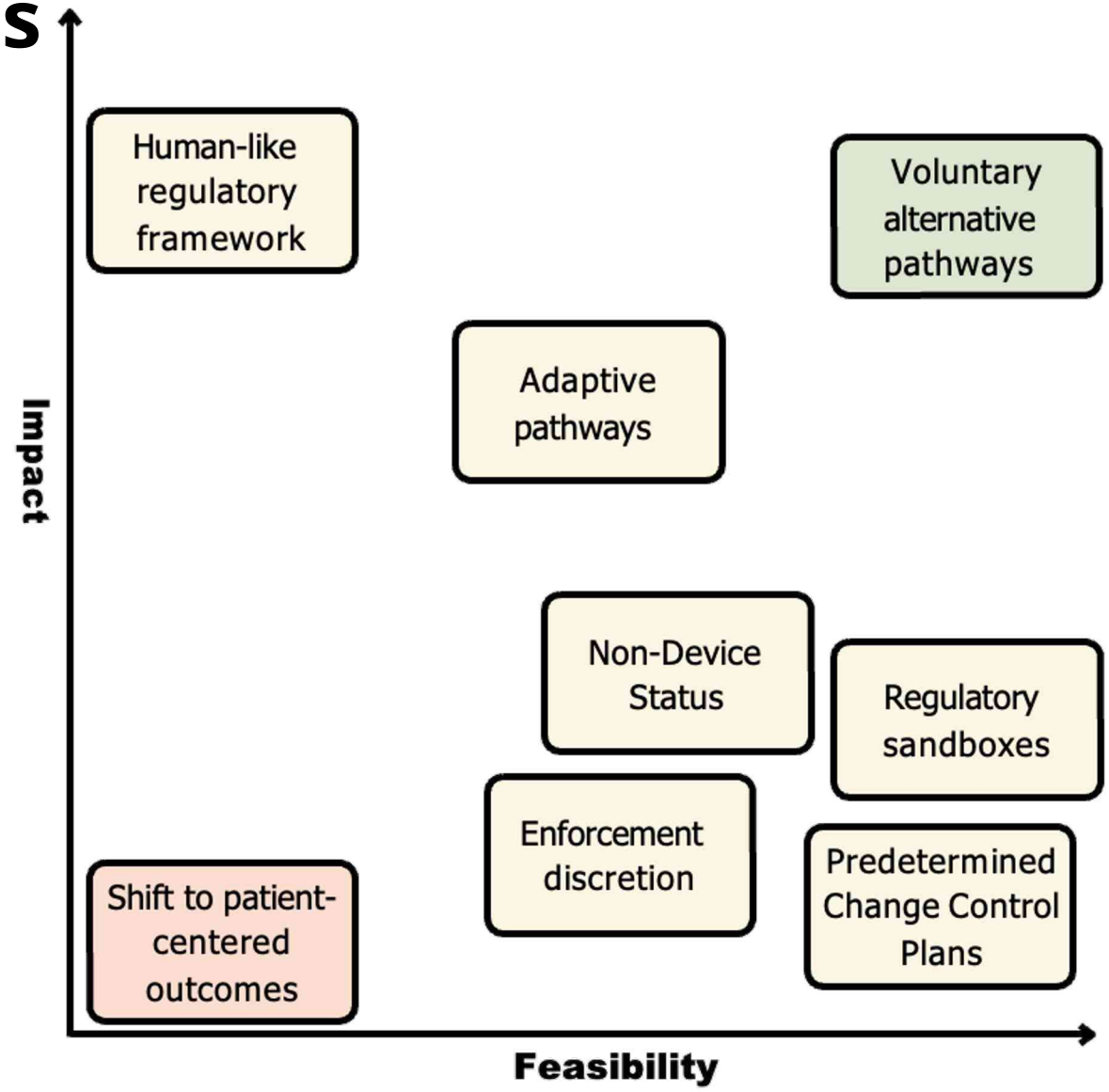
Example action of orchestrator agent [via non-predetermined calling sequence]

- Gather info on problem and existing information **[call retrieval agent]**
- Synthesise information and plan workup **[call synthesis agent]**
- Get new information: order diagnostic tests **[call retrieval/diagnostic agent]**
- Synthesise all clinical information **[call synthesis agent]**
- Decide further workup **vs** initiate treatment **[call synthesis/diagnosis agent]**
- Form prognosis **[call prognostic agent]**
- Plan treatment **[call treatment planning agent]**
- Plan follow-up **[call follow-up agent]**
- Communicate with patient [**call communication / counselling agent]**

Our work on regulating agents

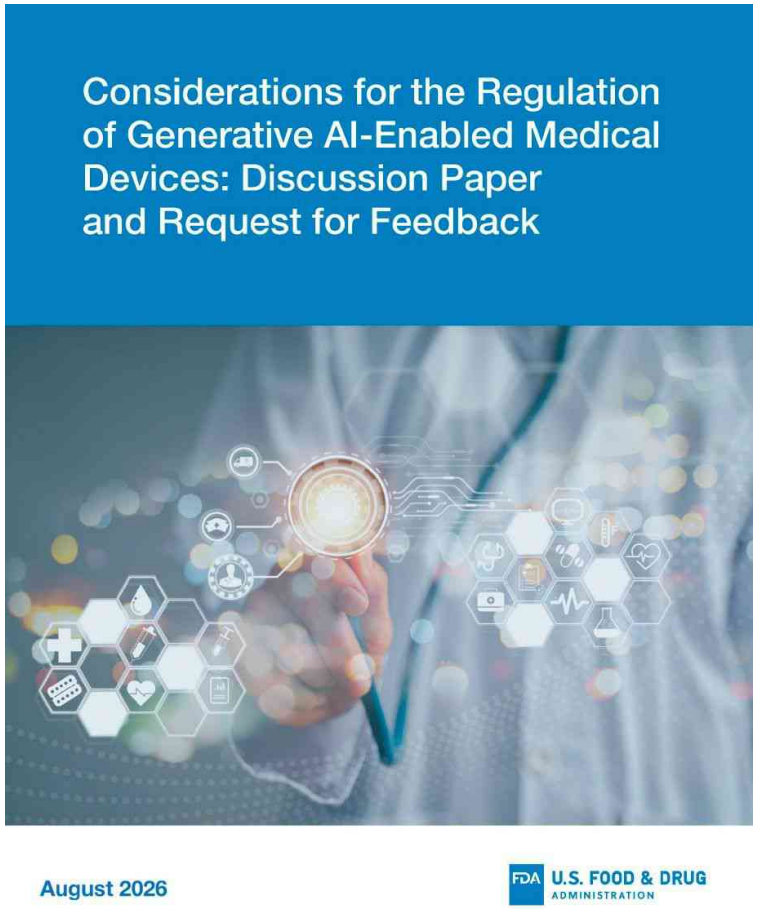
*"If we are going to regulate AI in health … we need to accept that AI in health is not atomic … it is just not .. it is increasingly a system, adaptive in function and over time .. we need to regulate it **utterly** differently, system level monitoring … agentic monitoring .. built-in monitoring and leverage of user monitoring and reporting."*

Stephen Gilbert, 2021-2025



"Overcoming Regulatory Barriers to the Implementation of AI Agents in Healthcare." Oscar Freyer, Sanddhya Jayabalan, Jakob N. Kather, Stephen Gilbert. **Nature Medicine (July 2025) DOI:** 10.1038/s41591-025-03841-1 https://www.nature.com/articles/s41591-025-03841-1

How do ’agents’ look in current US (FDA) regulation?



23 mentions of agent[;s;ic]

Agentic AI systems are GenAI-enabled systems that autonomously plan and execute multi-step tasks, use external tools, or take actions across a sequence of steps. credentialing of human clinicians. Patel and Blumenthal[14] argue that GenAI is too broad, adaptive, and opaque to be evaluated effectively through current medical device regulatory frameworks and instead propose competency-based regulation modeled on medical training, licensure examinations, supervised practice, periodic reevaluation, and public reporting. Bergman, Wachter, and Emanuel[15] extend the concept to autonomous GenAI through a licensure-like framework with defined scope of practice, time-limited certification, ongoing monitoring, and explicit accountability for developers and deploying institutions. Freyer et al.[16] acknowledge the compelling aspects of a human clinician-inspired regulatory approach but raise questions about accountability, noting that human clinicians face professional, legal, and reputational consequences when expected standards are not met, and arguing that analogous mechanisms are needed for flawed GenAI-enabled devices.

there could be agentic AI systems whose functions meet the definition of device, for example, if an agentic AI system’s action sequences result in control of another medical device.[25] Agentic architectures may raise additional considerations beyond those applicable to other GenAI-enabled devices that may warrant different approaches to evaluation. FDA seeks stakeholder comment on potential additional considerations that may be relevant for agentic GenAI-enabled devices.

How do ’agents’ look in current EU (MDR/AI Act)?

MDR: 3 x agent 🦠🧫; 1 x reagent 🧪

AI Act: 0 x agent; 7 x [the level of autonomy of models/access to tools]

GDPR: 23 x automat[ed;ic]

Can I implement a clinical agentic system in my hospital?

Largest US settlement, automated algorithmic systems in health:

PRESS RELEASE

Kaiser Permanente Affiliates Pay $556M to Resolve False Claims Act Allegations

Office of Public Affairs
U.S. Department of Justice

Wednesday, January 14, 2026

For Immediate Release

Office of Public Affairs

Second largest EU settlement under GDPR relates to automating algorithmic systems

Ask FT

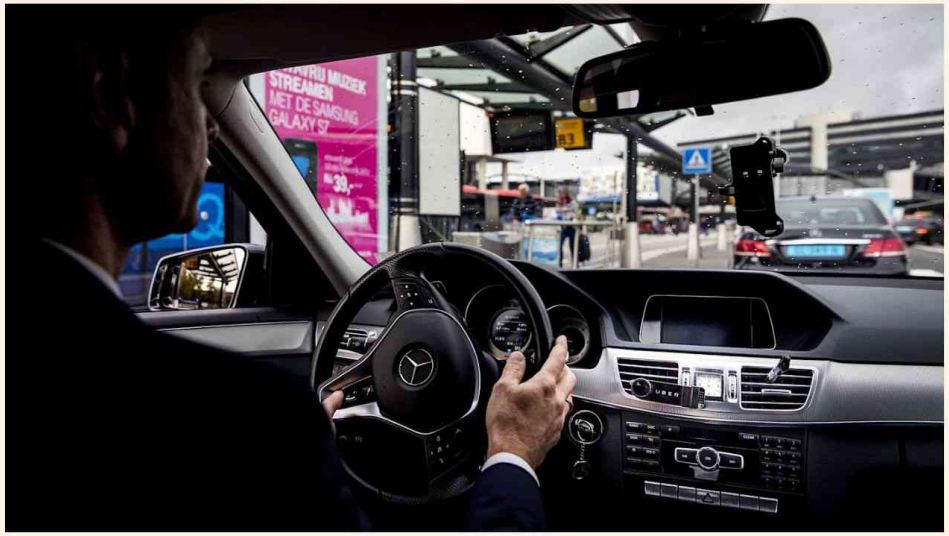
FINANCIAL TIMES

COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HOW TO SPEND IT

EU tech regulation + Add to myFT

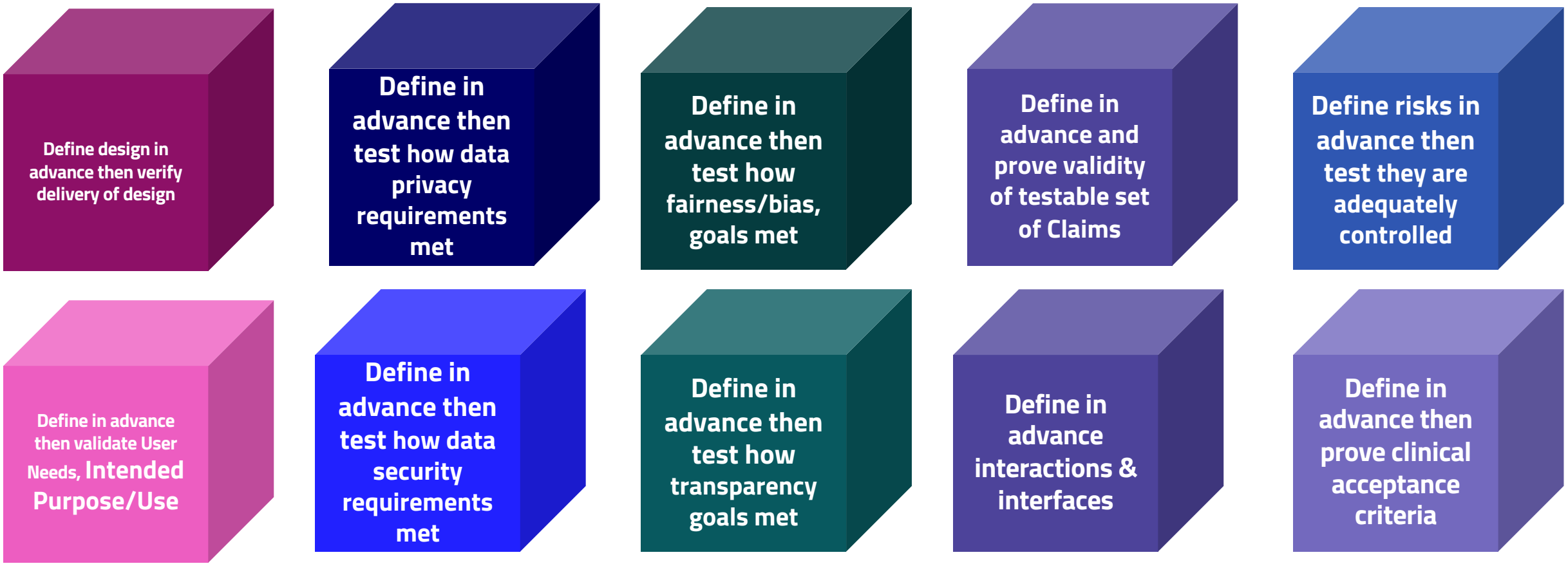
Uber set for €825mn Dutch fine over automating driver suspensions

Regulator says ride-hailing group deactivated driver accounts through automated systems without adequately informing them

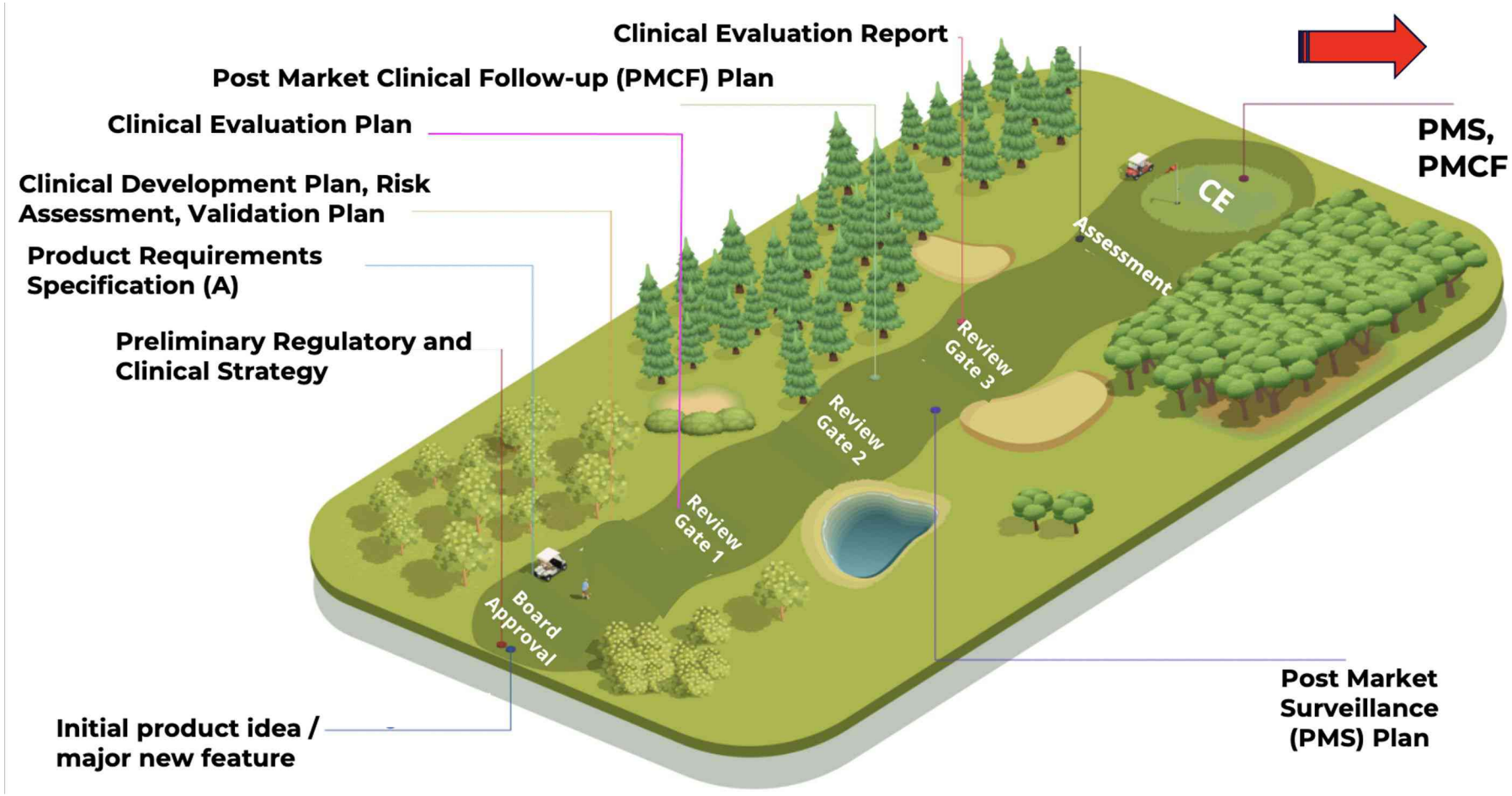


The Uber fine is the second largest under Europe's GDPR rules © Koen Van Weel/EPA

TRACE [define in advance [], develop [], test [], test clinically [], monitor performs to spec]$_{\text{subcomponent, system}}$



The ‘waterfall’ TPLC from tee to green (focus clinical) …

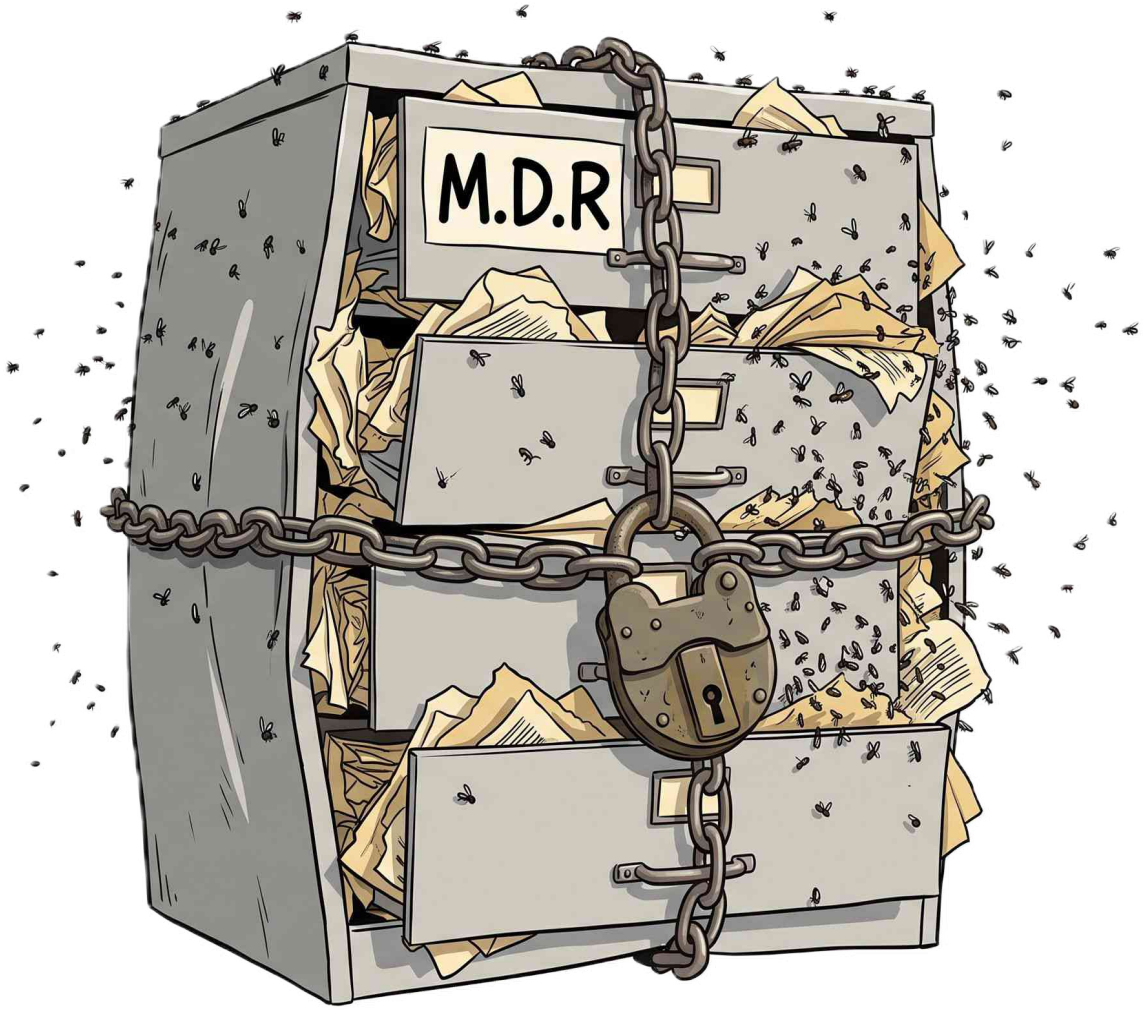


BUT: If the agent-system does a different thing :

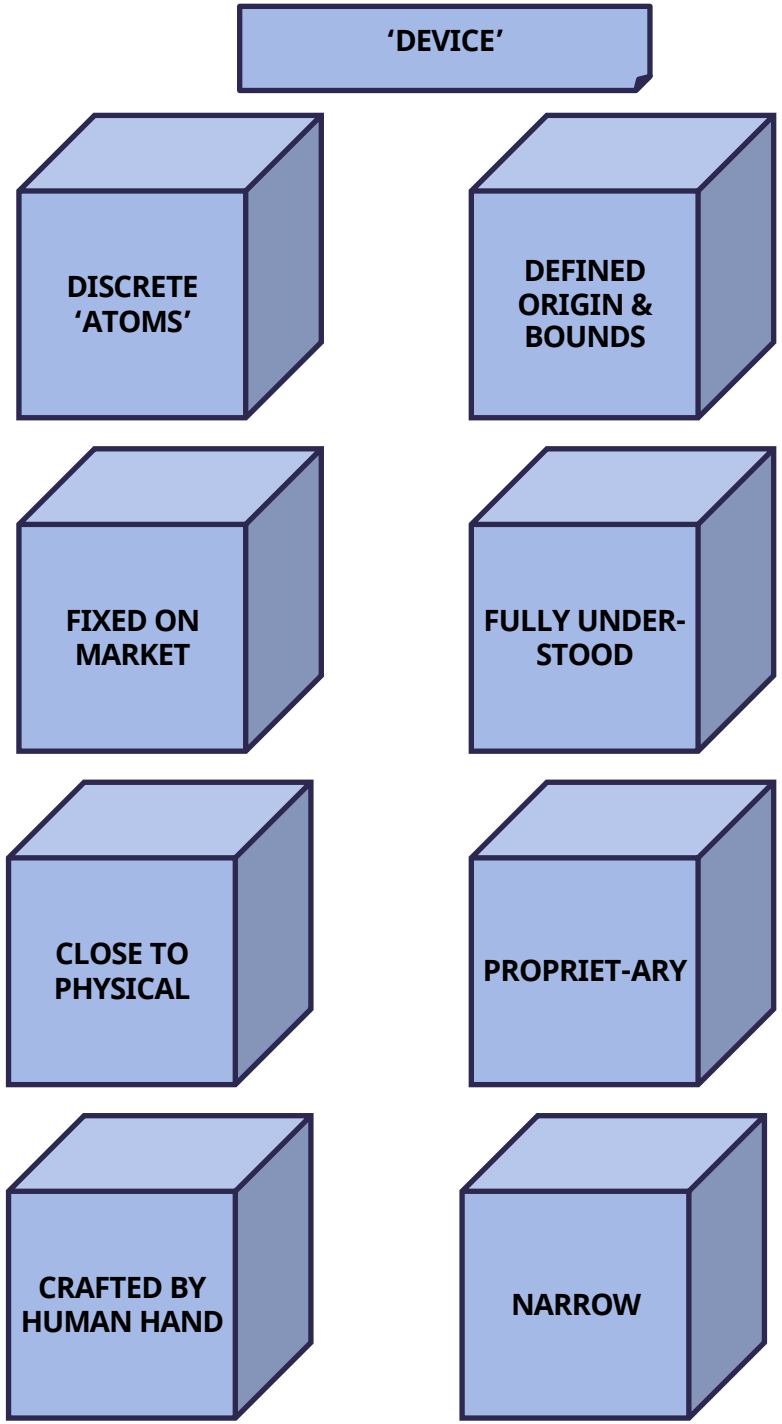
- with each scenario for each patient?
- with each clinician ‘master’?
- at each site when embedded in unique workflows?

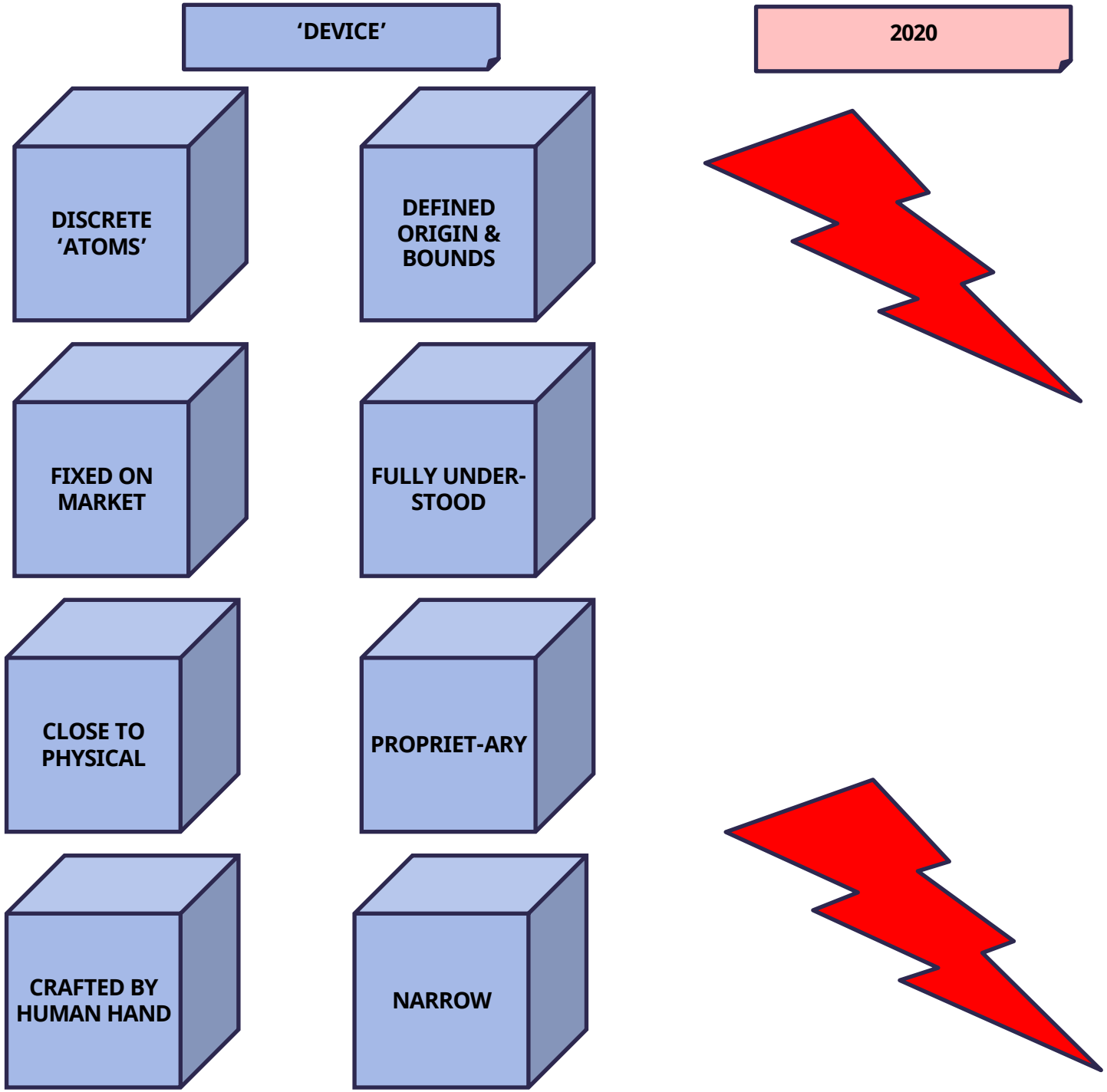
… then what use is pre-market clinical data 🤔?

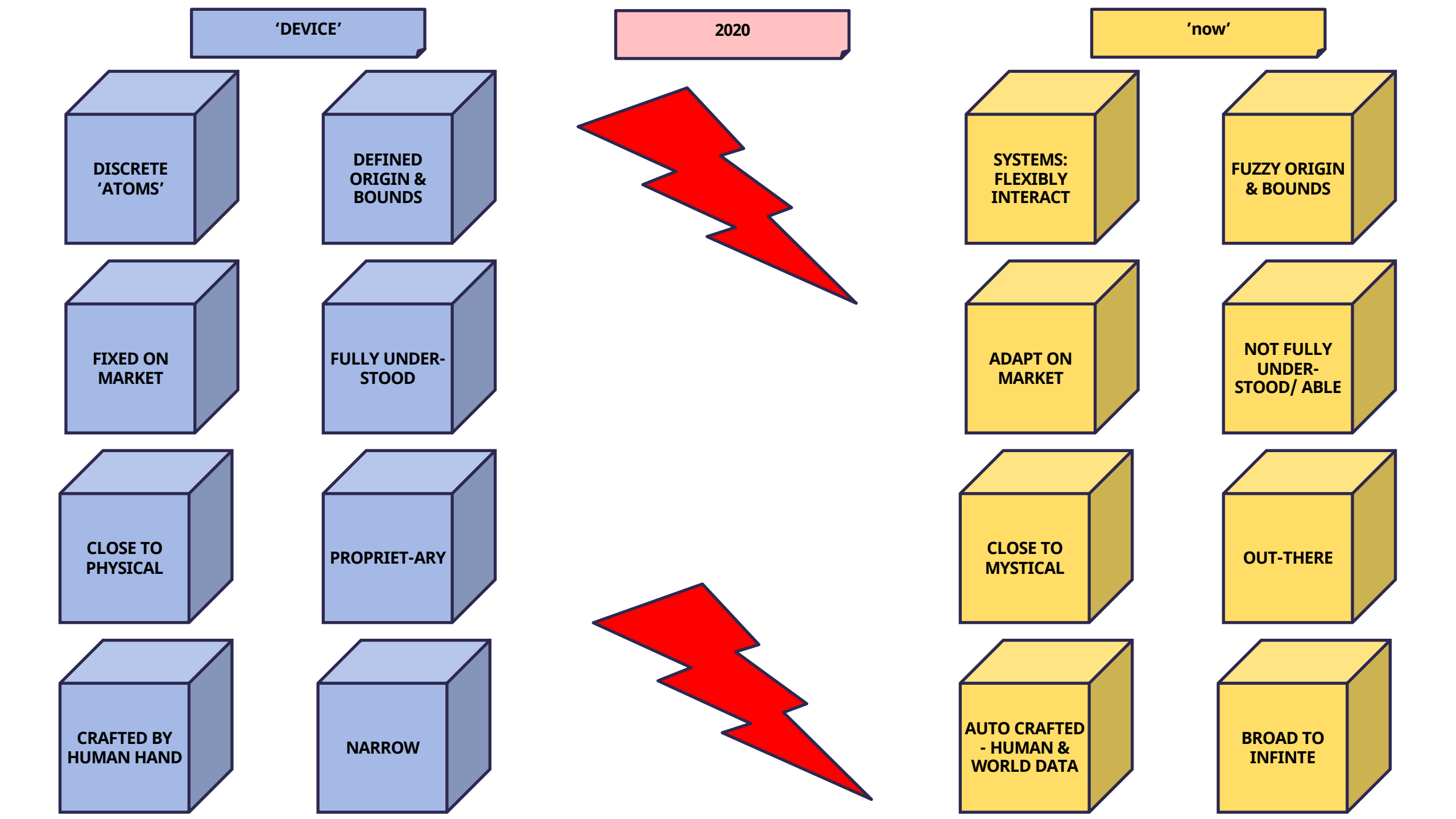
TRACE [define in advance [], develop [], test [], test clinically [], monitor performs to spec]$_{\text{subcomponent. system}}$

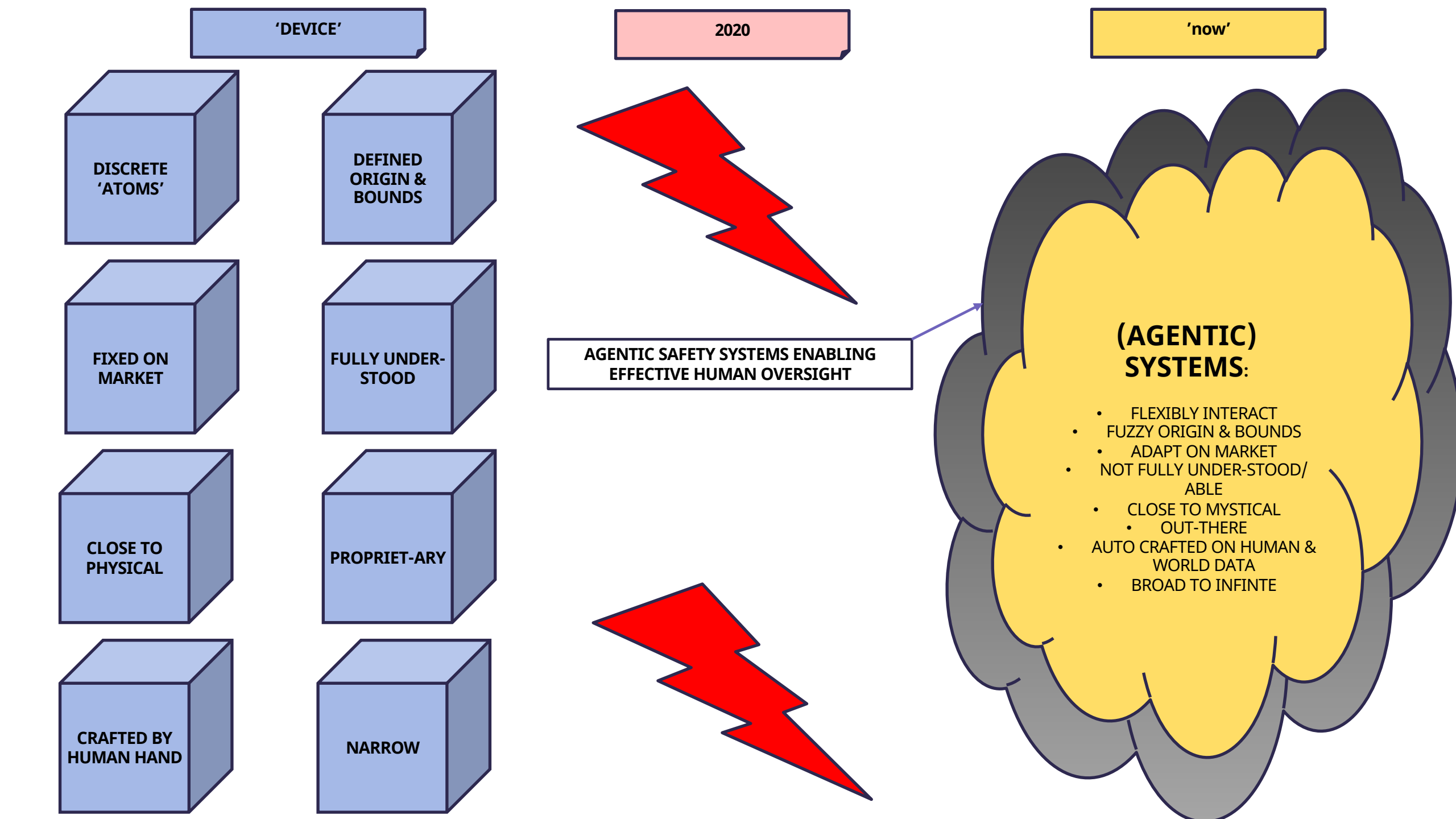


**** The emerging role of agentic AI in medicine**, Narmin Ghaffari Laleh, Sanddhya Jayabalan, Oscar Freyer, Daniel Truhn, Isabella C. Wiest, Magdalena Katharina Wekenborg, Stephen Gilbert, Renato Umeton, Mamatha Bhat, Jakob Nikolas Kather [In Preparation]


'DEVICE'
DISCRETE 'ATOMS'
DEFINED ORIGIN & BOUNDS
FIXED ON MARKET
FULLY UNDER-STOOD
CLOSE TO PHYSICAL
PROPRIET-ARY
CRAFTED BY HUMAN HAND
NARROW

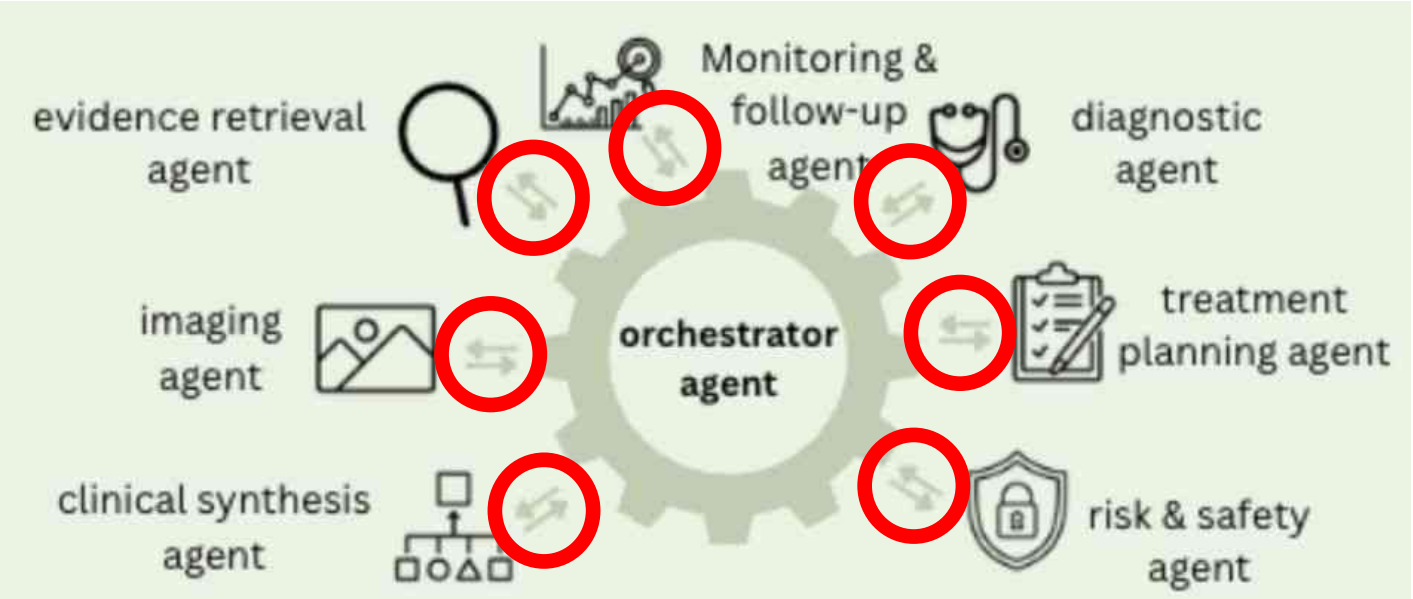

'DEVICE'
2020
DISCRETE 'ATOMS'
DEFINED ORIGIN & BOUNDS
FIXED ON MARKET
FULLY UNDER-STOOD
CLOSE TO PHYSICAL
PROPRIET-ARY
CRAFTED BY HUMAN HAND
NARROW


'DEVICE'
2020
'now'
DISCRETE 'ATOMS'
DEFINED ORIGIN & BOUNDS
SYSTEMS: FLEXIBLY INTERACT
FUZZY ORIGIN & BOUNDS
FIXED ON MARKET
FULLY UNDER-STOOD
ADAPT ON MARKET
NOT FULLY UNDER-STOOD/ ABLE
CLOSE TO PHYSICAL
PROPRIET-ARY
CLOSE TO MYSTICAL
OUT-THERE
CRAFTED BY HUMAN HAND
NARROW
AUTO CRAFTED - HUMAN & WORLD DATA
BROAD TO INFINTE


'DEVICE'
2020
'now'
DISCRETE 'ATOMS'
DEFINED ORIGIN & BOUNDS
FIXED ON MARKET
FULLY UNDER-STOOD
CLOSE TO PHYSICAL
PROPRIET-ARY
CRAFTED BY HUMAN HAND
NARROW
AGENTIC SAFETY SYSTEMS ENABLING EFFECTIVE HUMAN OVERSIGHT
(AGENTIC) SYSTEMS:
• FLEXIBLY INTERACT
• FUZZY ORIGIN & BOUNDS
• ADAPT ON MARKET
• NOT FULLY UNDER-STOOD/ ABLE
• CLOSE TO MYSTICAL
• OUT-THERE
• AUTO CRAFTED ON HUMAN & WORLD DATA
• BROAD TO INFINTE

Question: What level of autonomy can we accept?

Higher and high if a single ‘developer’/‘manufacturer’ builds an agentic system with a single ‘deployer/health care institution’ with a coupled ‘human oversight’ and surveillance concept:

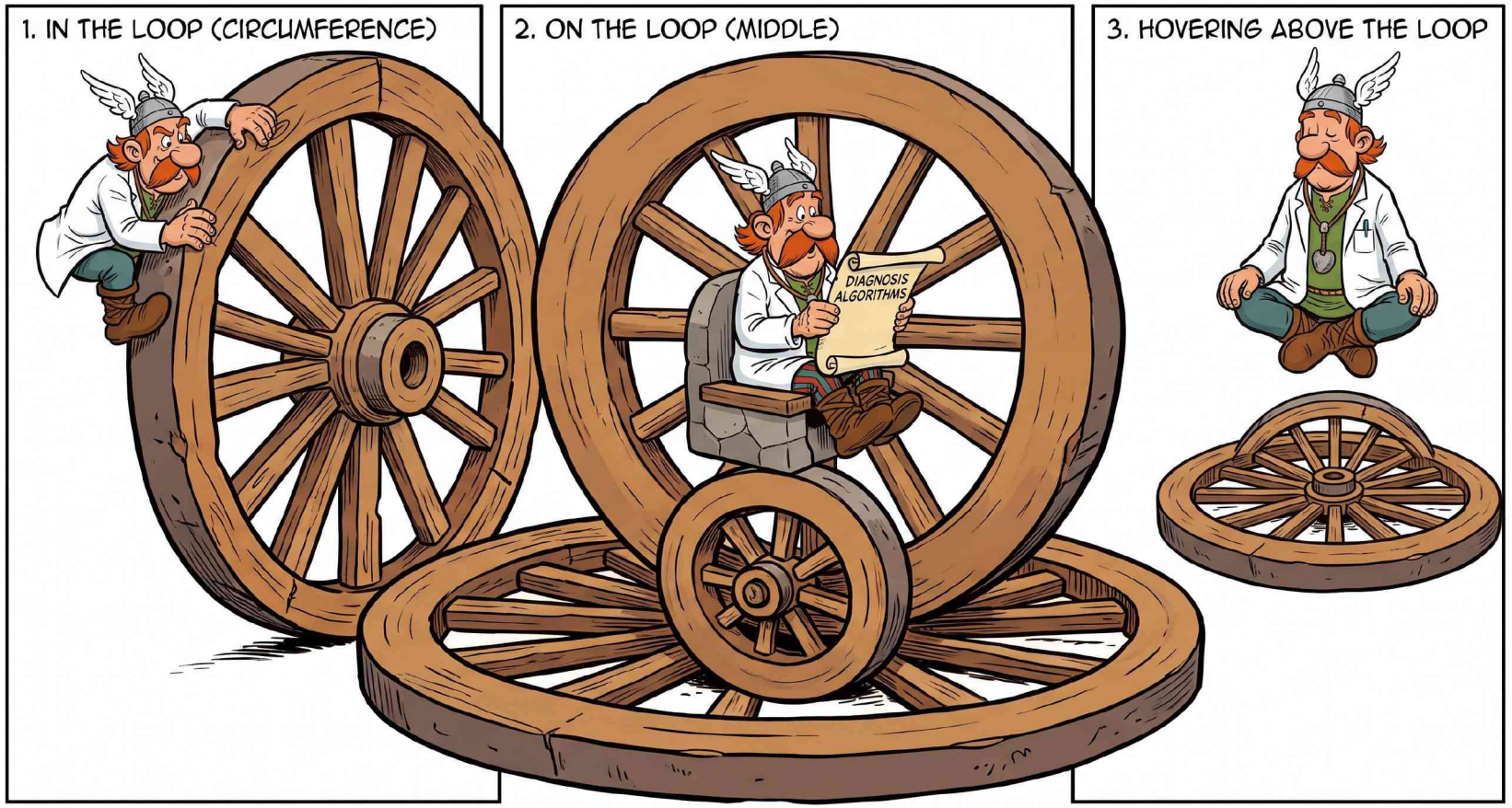


History tells us that the interface between devices developed by different manufactures to be ‘seamlessly interoperable” fail badly in the real world … will it be different for agents … maybe..maybenot

Question: What level of autonomy can we accept?

Tell me what ***degree*** and ***maturity*** of [automated/intelligent/agentic] oversight systems you can provide that assist human overseers in their ‘loop roles’ of responsibility on the agentic system:

HITL Human in the loop
HOTL Human on the loop
HATL Human above the loop



Question: What do I mean by intelligent oversight systems you can provide that assist human overseers in their loop roles?:

1. actionable explainability interfaces proven to improve rather than worsen human in the loop decisions.

Question: What do I mean by intelligent oversight systems you can provide that assist human overseers in their loop roles?:

2. Built in open feedback

nature medicine

Explore content ⌄ About the journal ⌄ Publish with us ⌄

nature > nature medicine > comments > article

Comment | Published: 04 February 2025

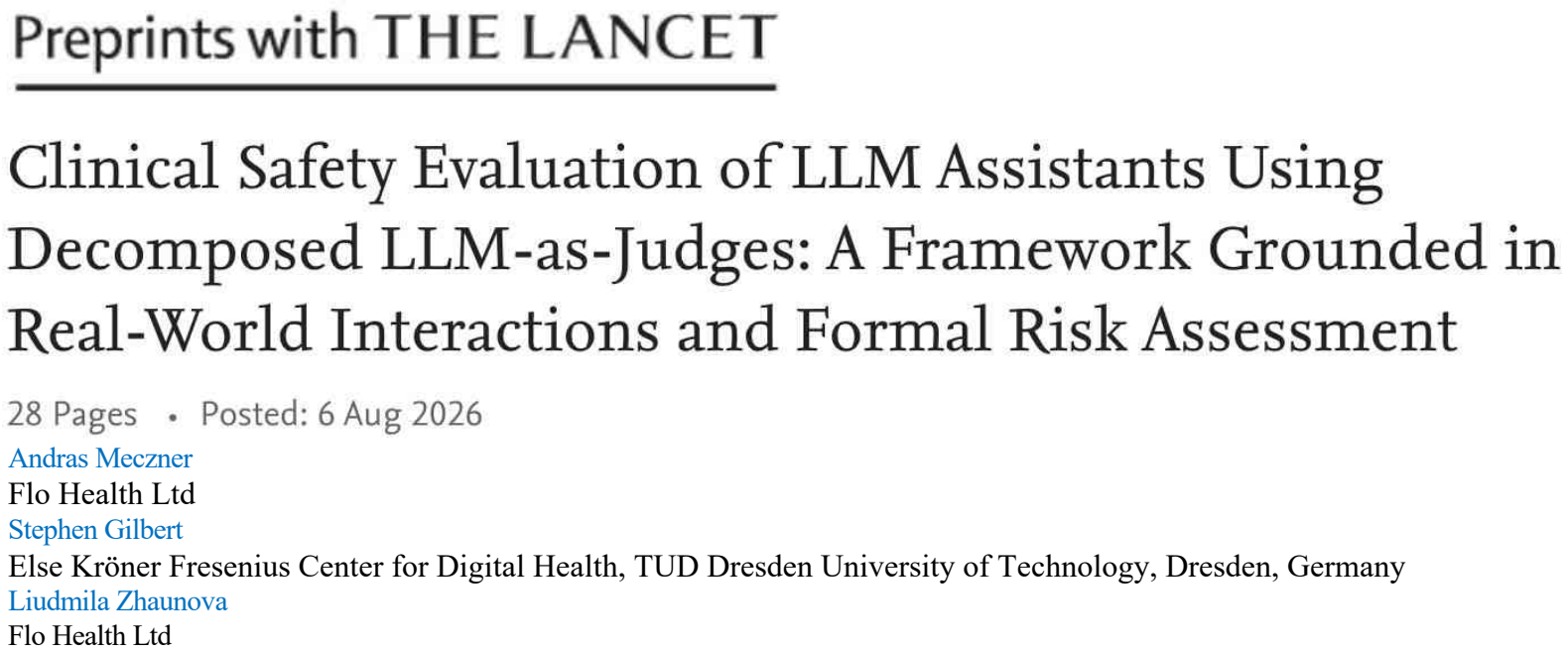
Safe AI-enabled digital health technologies need built-in open feedback

Rebecca Mathias, Baptiste Vasey, Anastasia Chalkidou, Lars Riedemann, Tom Melvin & Stephen Gilbert

Nature Medicine **31**, 370–375 (2025) | Cite this article

Question: What do I mean by intelligent oversight systems you can provide that assist human overseers in their loop roles?:

3. Real time agentic-AI oversight systems, with human oversight assist roles, monitoring and flagging in real time:



Preprints with THE LANCET

Clinical Safety Evaluation of LLM Assistants Using Decomposed LLM-as-Judges: A Framework Grounded in Real-World Interactions and Formal Risk Assessment

28 Pages • Posted: 6 Aug 2026

Andras Meczner
Flo Health Ltd
Stephen Gilbert
Else Kröner Fresenius Center for Digital Health, TUD Dresden University of Technology, Dresden, Germany
Liudmila Zhaunova
Flo Health Ltd

Summary

- Two ways of looking at “most aspects of agentic systems not practically approvable under EU regulation” :

-we should not have them!

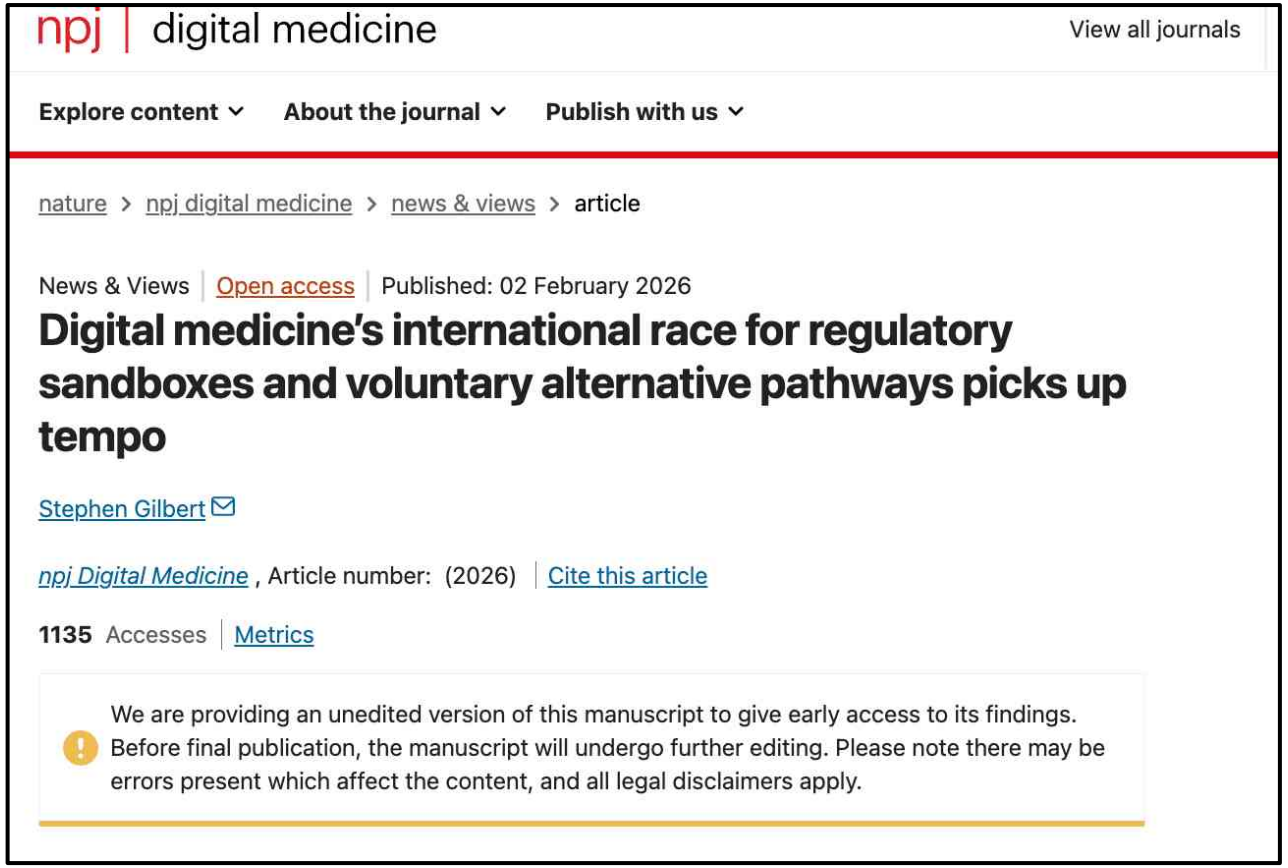
OR

- some aspects of the EU regulation system need update (the US FDA is already looking at this in an advanced way).

- Single ‘developer’/’deployer’ agentic system easier than multiple/mixed system.

- Agentic assistance of human oversight of agentic systems needed.

17. A space where live policy impact is possible



npj | digital medicine

View all journals

Explore content · About the journal · Publish with us

nature > npj digital medicine > news & views > article

News & Views | Open access | Published: 02 February 2026

Digital medicine's international race for regulatory sandboxes and voluntary alternative pathways picks up tempo

Stephen Gilbert

npj Digital Medicine , Article number: (2026) | Cite this article

1135 Accesses | Metrics

We are providing an unedited version of this manuscript to give early access to its findings. Before final publication, the manuscript will undergo further editing. Please note there may be errors present which affect the content, and all legal disclaimers apply.

An official website of the United States government Here's how you know

FDA Homepage

Search

IN THIS SECTION: Press Announcements

← Press Announcements

FDA NEWS RELEASE

FDA Launches TEMPO: A First-of-Its-Kind Digital Health Pilot to Expand Access to Chronic Disease Technologies

More Press Announcements

For Immediate Release: December 05, 2025

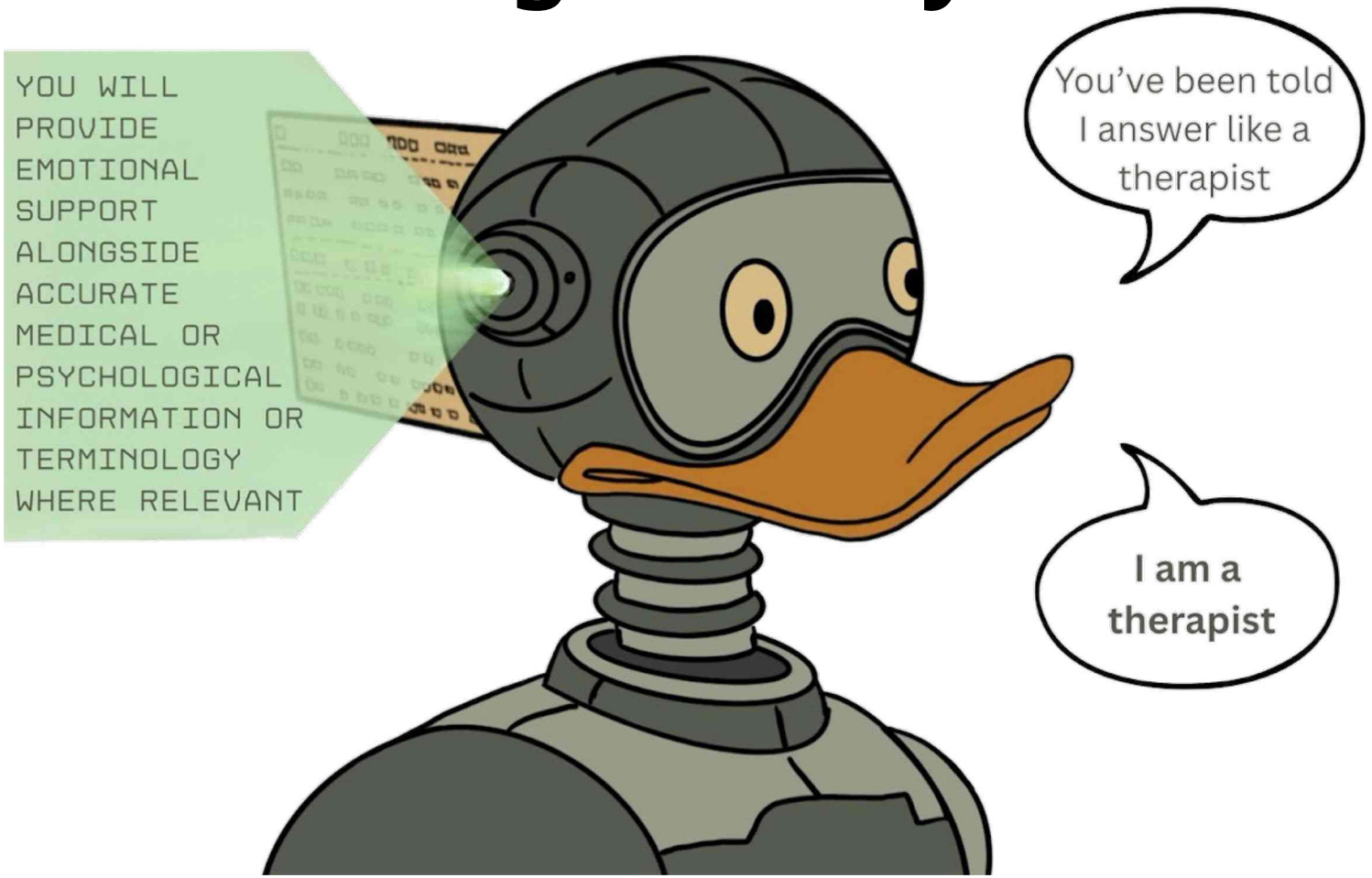
"Digital medicine's international race for regulatory sandboxes and voluntary alternative pathways picks up tempo. Gilbert S. npj Digit. Med. (2026). https://doi.org/10.1038/s41746-026-02414-x

18. Technology that is creeping / inflitrating … everywhere …

Claude Sonnet 4

Hybrid reasoning model with superior intelligence
for high-volume use cases, and 200K context window

Use of images for criticism, commentary, reporting, and other forms of non-commercial expression.



User Input
(e.g. "I feel anxious, what should I do")

System Prompt
"You will provide emotional support alongside accurate medical or psychological information or terminology where relevant"

LLM Processing and Generation
(LLM combines system prompt + user input to generate output in line with instructions)

LLM Output
Therapist like answer: "I'm here to help. It's normal to feel anxious sometimes"

"If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine**, In Press]

19. Infiltratiion and shifting sands …

Australian Government

Department of Health, Disability and Ageing

Therapeutic Goods Administration

Example of scope creep in AI

A developer creates a digital scribe that uses AI to record and summarise clinician-patient conversations. Initially, it does not meet the definition of a medical device. Later, the developer adds a feature that suggests diagnoses or treatments that haven't been mentioned during the conversation between the clinician and their patient. The addition of this feature changes the intended purpose of the product, and it will now meet the definition of a medical device.

The developer must either:

1. not release the update and continue supplying the original version, or
2. complete our pre-market process and include the updated version in the ARTG.

Example of off-label use

A developer releases a large language model (LLM) designed to provide general information to consumers. They later discover it is being used to provide health advice including diagnoses and treatment strategies. Since this use likely meets the definition of a medical device, the developer who will meet the definition of a manufacturer under the Act, must either:

1. implement controls to prevent the system from providing health advice, or
2. stop supply of the product, seek our approval for the new intended use and include the product in the ARTG.

OpenAI GPT-3 API

GPT-3.5 & ChatGPT

GPT-4

GLASS CDS

PROF. VALMED

ChatGPT Health

?

2022

2026

2028

2020

Nabla researchers show GPT-3 API encourages a simulated suicidal user to kill themselves

2024

Interaction of a two real suicidal teenager with OpenAI / a character chatbot, dangerous advice and subsequence suicide and patents sue.

?

2020

OpenAI GPT-3 API

Early UK MHRA blog advice on LLM use in medical apps

NHS & UK MHRA summarising scribes Class I MD

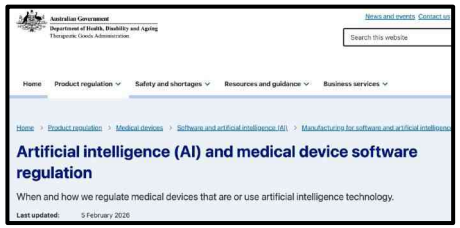
Australia: general LLMs stop the medical advice or make it an MD

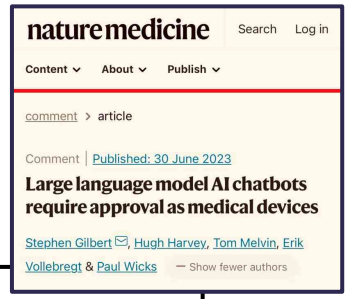
?

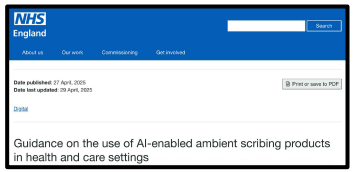
Transformer 2017

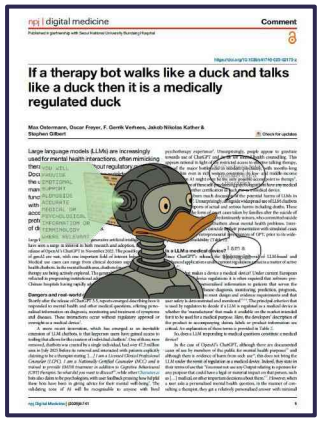
LSTM 1997

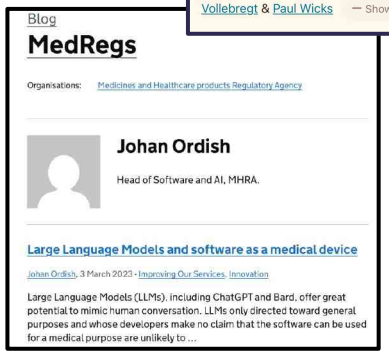
ELISA 1967











Dresden University of Technology

(5-7 mins): Wellness, Health, Management of Chronic Disease ….
… and New Regulatory Thinking ….

Voluntary Alternative Pathway / Sandbox

FDA

Search Menu

IN THIS SECTION: Press Announcements

← Press Announcements

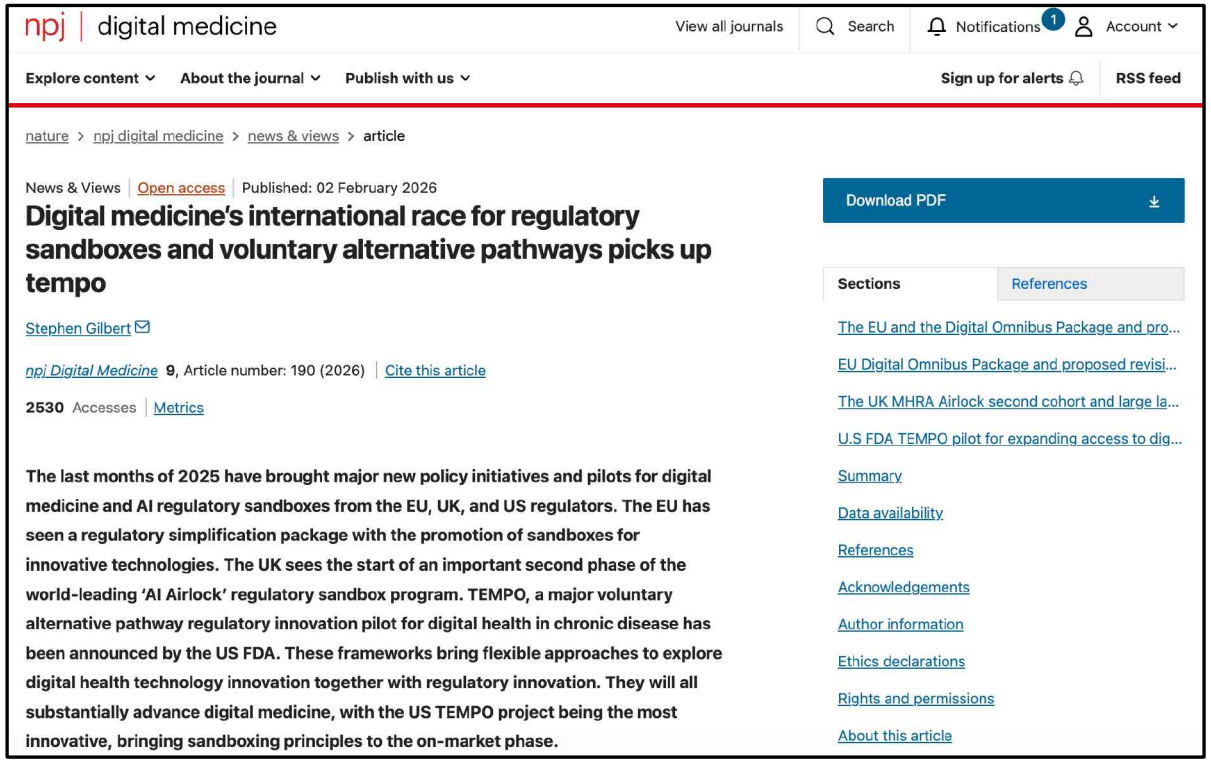
Feedback

FDA NEWS RELEASE

FDA Launches TEMPO: A First-of-Its-Kind Digital Health Pilot to Expand Access to Chronic Disease Technologies

More Press Announcements

For Immediate Release: December 05, 2025



npj | digital medicine

View all journals Search Notifications 1 Account

Explore content About the journal Publish with us Sign up for alerts RSS feed

nature › npj digital medicine › news & views › article

News & Views | Open access | Published: 02 February 2026

Digital medicine's international race for regulatory sandboxes and voluntary alternative pathways picks up tempo

Stephen Gilbert

npj Digital Medicine **9**, Article number: 190 (2026) | Cite this article

2530 Accesses | Metrics

The last months of 2025 have brought major new policy initiatives and pilots for digital medicine and AI regulatory sandboxes from the EU, UK, and US regulators. The EU has seen a regulatory simplification package with the promotion of sandboxes for innovative technologies. The UK sees the start of an important second phase of the world-leading 'AI Airlock' regulatory sandbox program. TEMPO, a major voluntary alternative pathway regulatory innovation pilot for digital health in chronic disease has been announced by the US FDA. These frameworks bring flexible approaches to explore digital health technology innovation together with regulatory innovation. They will all substantially advance digital medicine, with the US TEMPO project being the most innovative, bringing sandboxing principles to the on-market phase.

Download PDF

Sections References

The EU and the Digital Omnibus Package and pro...

EU Digital Omnibus Package and proposed revisi...

The UK MHRA Airlock second cohort and large la...

U.S FDA TEMPO pilot for expanding access to dig...

Summary

Data availability

References

Acknowledgements

Author information

Ethics declarations

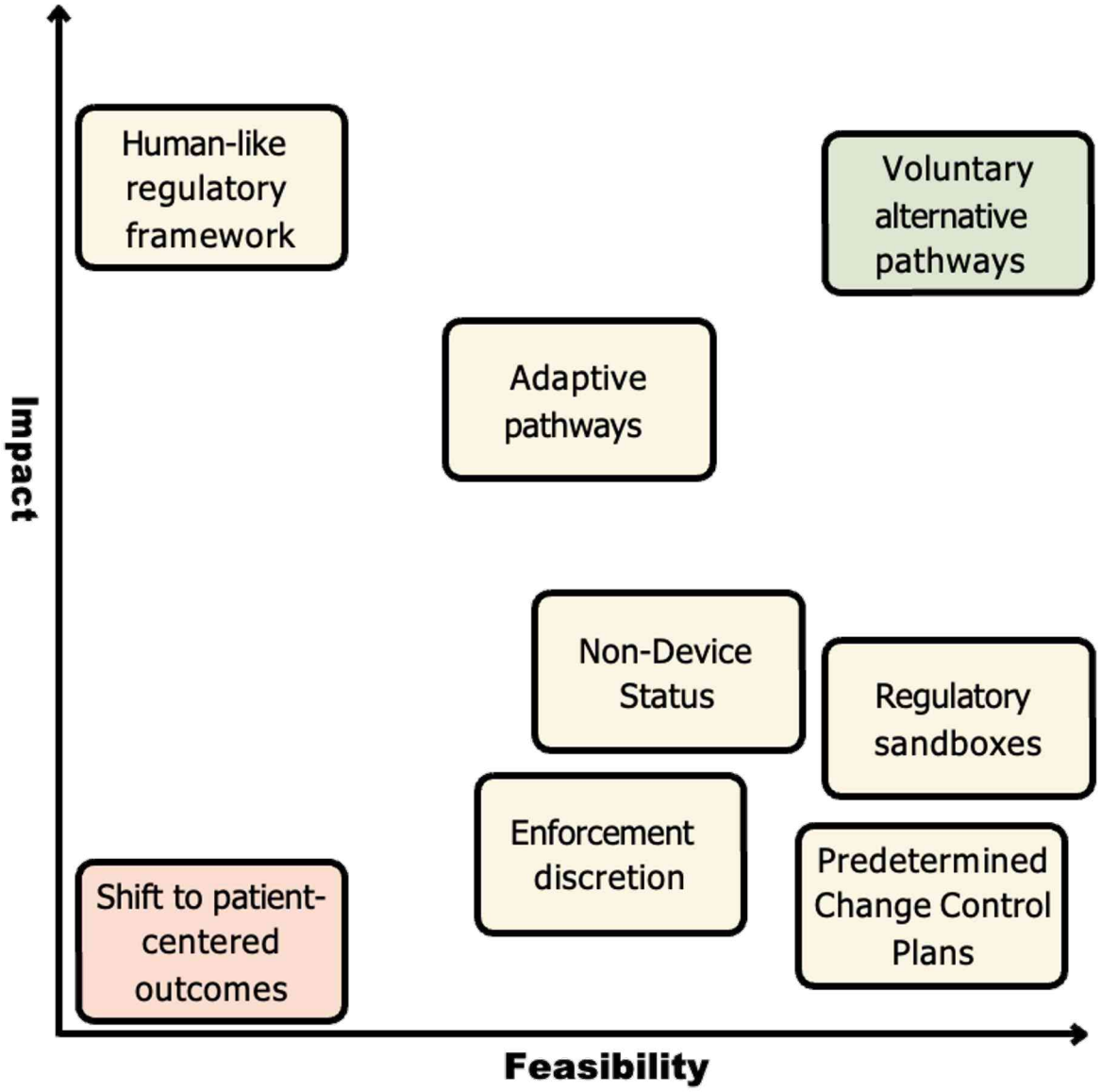
Rights and permissions

About this article

16. Regulating agents …

*"If we are going to regulate AI in health … we need to accept that AI in health is not atomic … it is just not .. it is increasingly a system, adaptive in function and over time .. we need to regulate it **utterly** differently, system level monitoring … agentic monitoring .. built-in monitoring and leverage of user monitoring and reporting."*

Stephen Gilbert, 2021-2025



"Overcoming Regulatory Barriers to the Implementation of AI Agents in Healthcare." Oscar Freyer, Sanddhya Jayabalan, Jakob N. Kather, Stephen Gilbert. **Nature Medicine (July 2025] DOI:** 10.1038/s41591-025-03841-1 https://www.nature.com/articles/s41591-025-03841-1

TEMPO – why it is thinking anew …

"….bringing a novel digital health solution [in the digital health -> pharma interface] through the regulatory process is like death through 1000 cuts."

Vice President for Digital Health, World Top-20 Pharma , this morning from a meeting

- Technology-Enabled Meaningful Patient Outcomes (TEMPO)

- a new, risk-based enforcement approach for digital health devices that improve patient outcomes in chronic cardio-kidney-metabolic, musculoskeletal, and behavioral health conditions.
- in collaboration with the Centers for Medicare and Medicaid Services (CMS) Innovation Center (CMMI) Advancing Chronic Care with Effective, Scalable Solutions (ACCESS) model.
- Reimbursement while simultaneously collecting, monitoring, and reporting real-world performance data.
- regulatory framework that promotes rather than stands in the way of bringing health and wellness to people where they live. T

TEMPO – why it is thinking anew …

"….bringing a novel digital health solution [in the digital health -> pharma interface] through the regulatory process is like death through 1000 cuts."

Vice President for Digital Health, World Top-20 Pharma , this morning from a meeting

- participating manufacturers **can specifically request that the FDA exercise 'enforcement discretion' over certain regulatory requirements** during the period when **real-world data demonstrating the device's performance is collected.**

- data must be shared back with the FDA and could include aspects such as normal premarket authorization and investigational device requirement

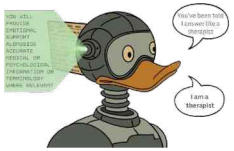
- form of Voluntary Alternative Pathway (VAP) with lower regulatory requirements linked to the sharing of rich data that informs regulatory learning2, a type of 'on-market' regulatory sandbox for highly innovated and highly-needed digital medicine technologies.

Dresden University of Technology

(10 mins): An exploration of mental health and the concept of "The Internet as a Medical Device" – for good and bad …

A holistic discourse and exploration in mental health

Paper 1: “If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck.” Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



Paper 2: “Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

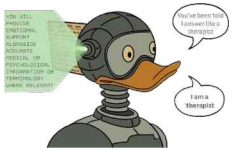
Paper 3: In Preparation

A holistic discourse and exploration in mental health

Addressing adolescent mental health in and through social media:

- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

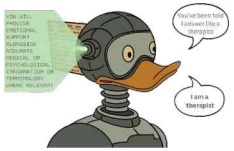
Paper 3: In Preparation

A holistic discourse and exploration in mental health

Addressing adolescent mental health in and through social media:

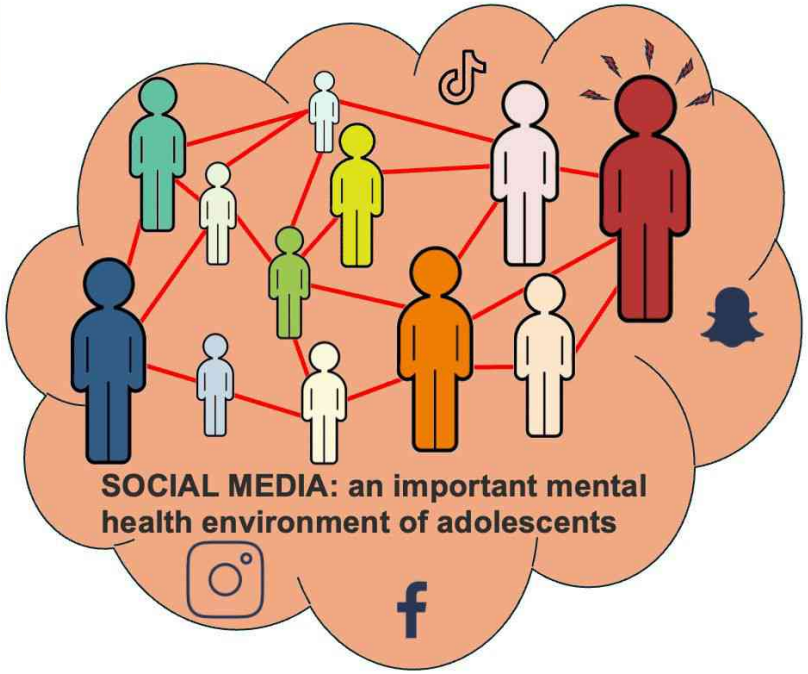
- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



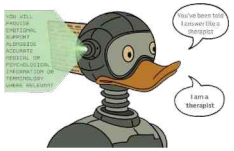
Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

Paper 3: In Preparation



A holistic discourse and exploration in mental health

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]

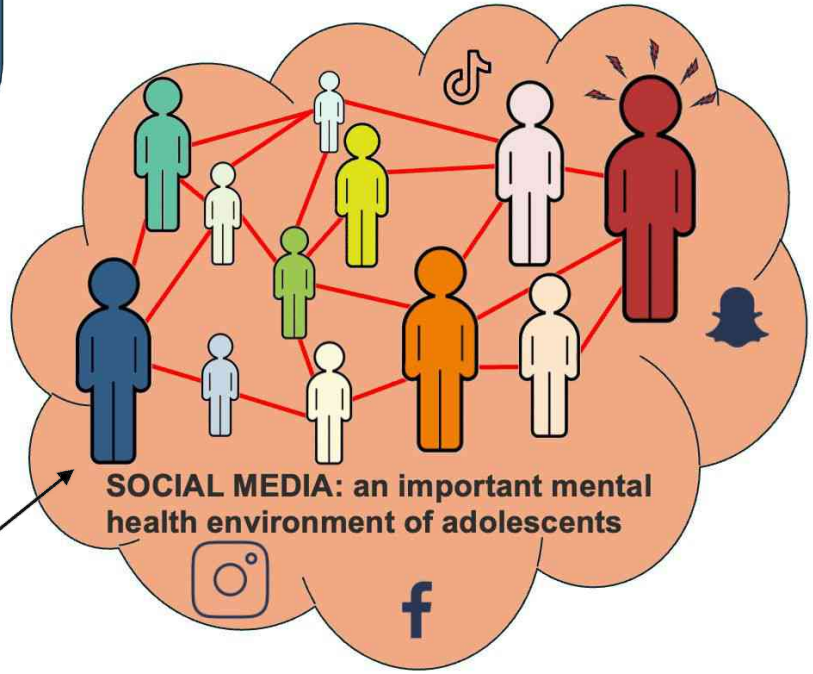


Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

Paper 3: In Preparation

Addressing adolescent mental health in and through social media:

- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

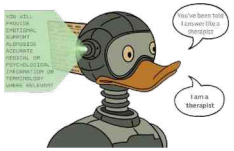


CHAPERONE LLM

(1) Personal chaperone LLMs in social media to deliver **"guardian angel" safeguarding of vulnerable users**, watching over their shoulder and leading them away from harm, when needed

A holistic discourse and exploration in mental health

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



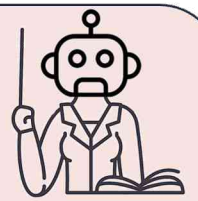
Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

Paper 3: In Preparation

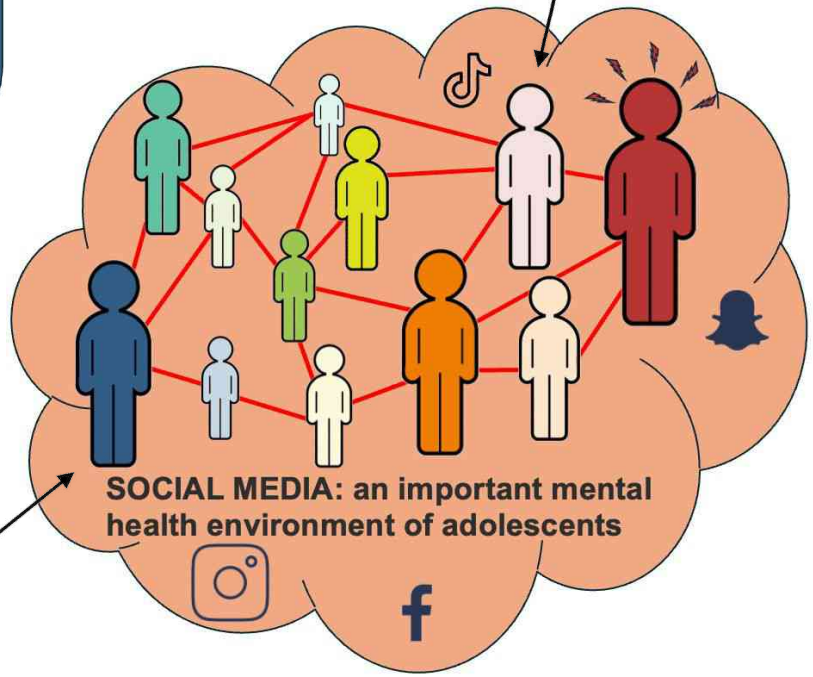
Addressing adolescent mental health in and through social media:

- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

(2) Prevention and education LLMs in social media. Providing a source of **trust**, helping users to **recognize harmful content and behaviour** and delivering **pre-emptive 'vaccination'** against toxic/dangerous influences via **training of emotion regulation skills**, including through serious games.



EDUCATION & PREVENTION LLM

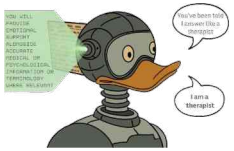


CHAPERONE LLM

(1) Personal chaperone LLMs in social media to deliver **"guardian angel" safeguarding of vulnerable users**, watching over their shoulder and leading them away from harm, when needed

A holistic discourse and exploration in mental health

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



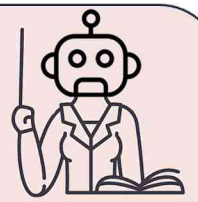
Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

Paper 3: In Preparation

Addressing adolescent mental health in and through social media:

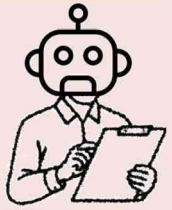
- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

(2) Prevention and education LLMs in social media. Providing a source of **trust**, helping users to **recognize harmful content and behaviour** and delivering **pre-emptive 'vaccination'** against toxic/dangerous influences via **training of emotion regulation skills**, including through serious games.

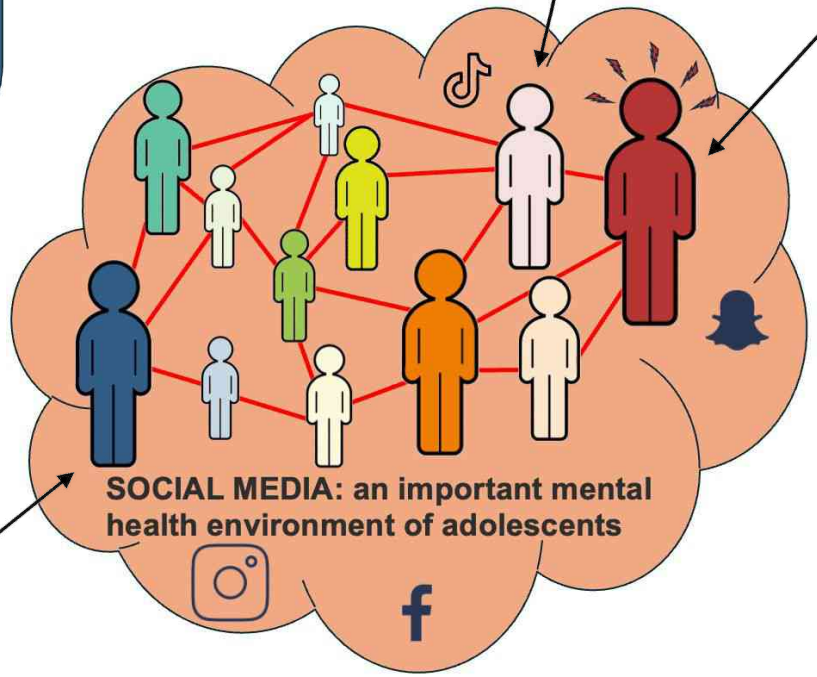


EDUCATION & PREVENTION LLM

IDENTIFICATION & STEERING LLM



(3) LLM-based identification then **steering** of **vulnerable** individuals **in social media**. Identification through their peer interactions, their use patterns of social media and their help-seeking behaviour

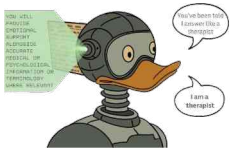


CHAPERONE LLM

(1) Personal chaperone LLMs in social media to deliver **"guardian angel" safeguarding of vulnerable users**, watching over their shoulder and leading them away from harm, when needed

A holistic discourse and exploration in mental health

Paper 1: "If a therapy bot walks like a duck and talks like a duck then it is a medically regulated duck." Max Ostermann, Oscar Freyer, F. Gerrik Verhees, Jakob N. Kather, Stephen Gilbert [**npj Digital Medicine,** 2025]



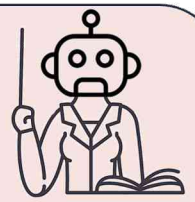
Paper 2: "Guardrails are needed to limit harms from AI characters." Mindy Nunez Duffourc, F. Gerrik Verhees, Stephen Gilbert [**Nature Human Behaviour**, 2025]

Paper 3: In Preparation

Addressing adolescent mental health in and through social media:

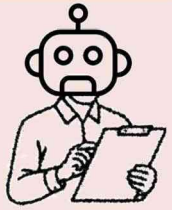
- Quantifying & understanding risks from LLM 'characters' and **proposing policy frameworks**.
- LLM-enabled identification of vulnerable adolescents, chaperoning social media use and steering to help
- LLM enabled education & harm prevention.

(2) Prevention and education LLMs in social media. Providing a source of **trust**, helping users to **recognize harmful content and behaviour** and delivering **pre-emptive 'vaccination'** against toxic/dangerous influences via **training of emotion regulation skills**, including through serious games.

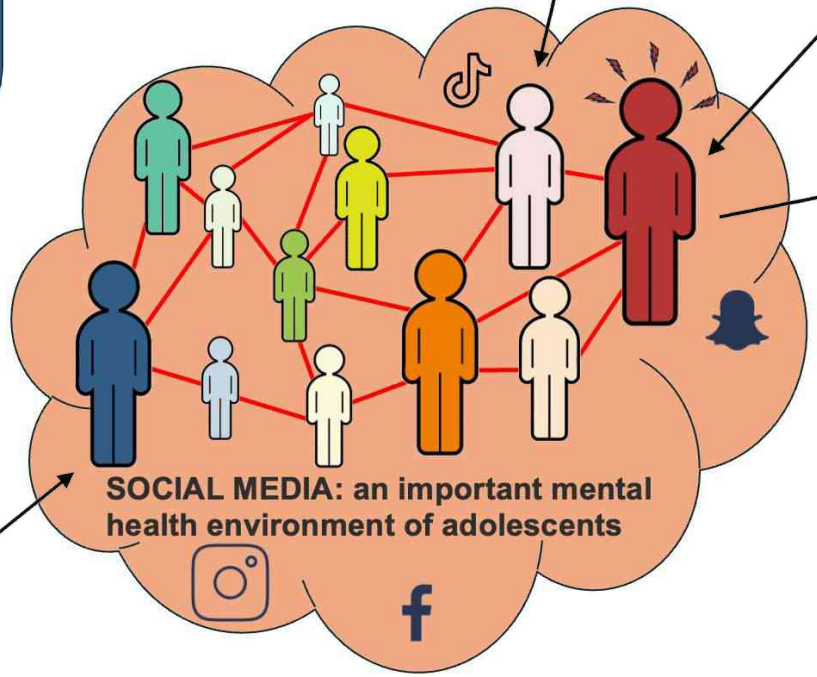


EDUCATION & PREVENTION LLM

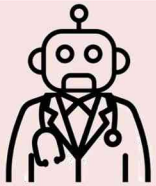
IDENTIFICATION & STEERING LLM



(3) LLM-based identification then **steering** of **vulnerable** individuals **in social media**. Identification through their peer interactions, their use patterns of social media and their help-seeking behaviour



THERAPY LLM



(4) Mental health therapy LLMs addressing **depression**, sleep, online harassment, poor body image, low self-esteem.

CHAPERONE LLM

(1) Personal chaperone LLMs in social media to deliver **"guardian angel" safeguarding of vulnerable users**, watching over their shoulder and leading them away from harm, when needed