

RB Weekly AI Brief - Issue 29 - 22.10.2026

Covering the week of 22.10.2026 · Issue 29 of the RB Weekly AI Brief

Recurring themes: Regulatory & HTA Signals (3 of last 4 issues) · Regulation & Policy (3 of last 4 issues) · Healthcare & Life Sciences (3 of last 4 issues) · Models & Research (3 of last 4 issues)

AI News Roundup

Regulation & Policy

AI-Found PHP Flaws Force Global Patch Scramble and Website Shutdowns

On 21 October the PHP project released fixes for two critical vulnerabilities that can allow unauthenticated remote code execution, each rated 9.2 on the CVSS v4.0 scale. The flaws had gone undetected for more than a decade. According to the BBC, they were found by researchers at Calif and Wiz using frontier AI tools, with Calif and the PHP Foundation taking part in OpenAI's Patch the Planet programme; OpenAI says an internal researcher found the issue around the same time. Details leaked on social media on 20 October, forcing PHP to announce early. Official fixes cover PHP 8.2 and later, with only source backports for older branches. The UK NCSC advised organisations that cannot remediate immediately to consider taking systems offline, and the US NSA gave similar advice. Finland's government web services, the Dutch NCSC, the Dutch National Institute for Public Health and the Environment and Wikimedia systems were among those taken offline. Wiz estimates that roughly 70 per cent of the internet is affected, a figure the BBC could not verify.

***So what?** PHP sits beneath WordPress, Drupal and a great deal of third-party software, often without organisations knowing, so the first task is an inventory, not a patch. Pharma and HEOR teams should ask IT and vendors whether patient-facing portals, trial and congress sites and vendor-hosted tools run PHP, whether they are patched, and whether any were taken offline. It is also a concrete example of AI finding critical flaws before attackers did, which cuts both ways for security planning.*

BBC News

UK to Consider Extending Cyber Bill to Serious AI Incidents and Near-Misses

On 12 October the UK government announced that it will consider stronger protections against emerging AI threats through the Cyber Security and Resilience Bill regime, with AI Minister Kanishka Narayan speaking at Imperial College London. It will examine how serious AI incidents and near-misses can be identified and reported, and how lessons can be learned quickly, with details to be worked out with parliamentarians, technical experts and operators. The release names essential services such as hospitals and utilities, and AI loss-of-control risk, where autonomous systems evade human oversight. The NCSC and the AI Security Institute are working on how incidents involving AI agents should be handled. The measures are described as first steps and no fixed deadlines are given. Privacy Laws & Business reports that the Bill reaches Report stage in the House of Lords on 26 October, with enactment expected in early 2027.

***So what?** This week's PHP shutdowns show why the proposal matters: essential services such as hospitals are being asked to plan for AI-related failures as well as conventional ones. Pharma and NHS-facing technology suppliers should expect incident-reporting expectations to extend to AI agents, and should check whether their own incident-response plans cover agentic failures and near-misses.*

UK Government

Anthropic Pitches Narrow Frontier-AI Safety Bill to US Lawmakers

Politico reported on 16 October, as carried by Reuters, that Anthropic has quietly pitched lawmakers a draft federal bill on frontier AI safety. Under the draft, the government could block a model's release or use only where it poses a foreseeable, imminent risk of more than \$1 billion in damages, or of killing or seriously injuring more than 50 people, arising from biological weapons, a model evading its developer's controls, or a cyberattack. The Commerce Department would have to ask a federal judge to halt a model, and the draft would bar other agencies from suspending development or deployment themselves. Independent evaluators would register with Commerce, could be paid by the labs provided payment is not tied to the outcome, and would have to report imminent risks to Commerce within 72 hours. An Anthropic spokesperson said the draft reflects its Advanced AI Framework. No sponsor or bill number has been reported.

So what? This is a vendor-written template for frontier model oversight: high thresholds, court-supervised halts and a registered evaluator regime. If anything like it advances, third-party evaluation reports could become standard procurement documents for pharma teams buying AI tools, and the threshold design would decide how much regulators can act before harm occurs. It is a pitch, not a bill.

Reuters (via The Star)

Regulatory & HTA Signals

EMA/HMA Notes Confirm AI Concept Paper Is Being Finalised Ahead of Consultation

Summary notes published on 14 October of the 5 October HMA-EMA focus-group meeting with industry stakeholders on AI in the medicines lifecycle say that a concept paper on AI in clinical development is being finalised and will be followed by public consultation. A horizontal guidance document on general machine-learning principles is also in progress, and the two are meant to progress in parallel and complement each other. The notes refer to the joint EMA-FDA AI glossary and the EMA-FDA guiding principles for good AI practice, with follow-up activities, and say that further discussions on AI collaboration between the European Commission, EMA and FDA are planned for November 2026. Industry speakers named in the notes include ACRO, Europharm SMC, EuropaBio, EUCOPE and MPA.

So what? The concept paper will set out how EMA expects AI to be used in clinical development, so sponsors using AI for trial design, endpoints or data analysis should prepare to respond to the public consultation. The parallel horizontal guidance suggests expectations will extend across the medicines lifecycle, which in turn shapes the evidence that HTA bodies see.

EMA

JHEOR Proposes TRACE-HEOR Reporting Standard for AI in Health Economic Models

Published on 15 October in the Journal of Health Economics and Outcomes Research, the second article in a 'Faster but Not Truer' series audits 1,391 HTA documents and finds three that disclose an AI component, about 0.2 per cent, all of them NICE technology appraisals. The audit measures disclosure, not use. The paper proposes TRACE-HEOR, a 10-item reporting standard extending CHEERS 2022 and PALISADE. Its 'decision reversal' item asks submitters to re-estimate the primary result with the AI component replaced by the pre-AI alternative or a plausible worst case, and to state whether the recommendation changes or the incremental cost-effectiveness ratio crosses the threshold. The author reports no documented case of a regulator or HTA body accepting or rejecting an AI-derived endpoint as such, based on a narrative review of the record through September 2026. TRACE-HEOR is offered as a starting draft and has not been through a consensus process.

So what? For HEOR teams, the decision-reversal item is the one to watch: it would require a counterfactual run of the economic model without the AI component. Teams already using AI in evidence synthesis or modelling could trial it now, as a way to document AI's contribution before any HTA body asks. It is a proposal, not a requirement.

Journal of Health Economics and Outcomes Research

Healthcare & Life Sciences

AstraZeneca and insitro Sign AI Drug Discovery Deal Worth Up to About \$1.5B

On 15 October AstraZeneca announced a strategic collaboration with insitro to discover treatments for metabolic dysfunction-associated steatohepatitis (MASH) and cardiomyopathies. insitro will apply its Virtual Human platform, which brings together large-scale human and cellular data, to identify causal disease biology and advance AstraZeneca-nominated targets to development candidates, while AstraZeneca uses its clinical development and regulatory expertise. AstraZeneca has exclusive worldwide rights to advance selected programmes. insitro receives \$40 million upfront and is eligible for up to about \$1.46 billion in development and commercial milestones, plus potential single-digit royalties on global sales. All terms are company-announced.

So what? The headline value is almost entirely milestones, so this is a bet on a platform rather than the purchase of an asset. HEOR and market access teams should treat it as an early signal of competitive interest in MASH and cardiomyopathy, and watch for the first development candidates, where differentiation and evidence plans will begin to matter.

AstraZeneca

AstraZeneca and Oracle Sign Non-Binding Term Sheet for AI-Enabled Clinical Trial Collaboration

On 20 October AstraZeneca and Oracle Health and Life Sciences announced a non-binding term-sheet agreement to use AI and deidentified real-world data to improve clinical trial recruitment, earlier diagnosis, drug-safety monitoring and real-world evidence across the lifecycle of a medicine. Programmes are to span AstraZeneca's core disease areas: oncology, cardiovascular, renal and metabolic diseases, respiratory and immunology, and rare disease. A first programme supports hypertension care and clinical research in Abu Dhabi, with the healthcare company M42. The companies say AstraZeneca will not receive patient-identifiable information and that each project will be reviewed separately before it proceeds. No financials were disclosed.

So what? Because the agreement is non-binding and carries no disclosed financial terms, treat it as a direction of travel. The governance detail is the part to note: deidentified data, project-by-project review and no patient-identifiable information reaching the sponsor are the safeguards likely to be expected of AI-enabled real-world evidence generation.

AstraZeneca

Models & Research

Meta Releases Muse Spark Open, Claiming Most Capable US Open-Weight Model

Meta Superintelligence Labs released Muse Spark Open on 15 October, a natively multimodal mixture-of-experts model with 816 billion parameters in total, 42 billion active per token and a one-million-token context window. Meta says it is the most capable US open-weight model to date, but its blog post gives no benchmark scores in the text and links to a separate evaluation report, so the claim is Meta's own. Meta also says the model can run on two Apple M5 Ultra Mac Studios using MLX. Weights are available on Hugging Face under the Muse Model License, which Meta describes as having limited commercial terms.

So what? For pharma and HEOR teams with sensitive data, a large open-weight model that can run on local hardware is worth evaluating, but the licence terms and independent benchmarks matter more than the headline claim. Check whether the licence permits your intended commercial use before any pilot.

Meta AI Research

Academic Paper Summaries

Selected from PubMed · Published within the last 12 months · New selections each week

Domain Paper — HEOR / Health Economics / Market Access

Integrating ethical analysis in health technology assessment: opportunities and challenges.

Bloemen B, Axler R, DiStefano MJ, et al. · International journal of technology assessment in health care · 2026

#HTA · #MarketAccess · #Regulation

This paper from the HTAi Interest Group for Ethical Issues in HTA reflects on why ethical analysis, long recognised as part of health technology assessment, has seen limited and challenging integration in practice. Drawing on a workshop and online meetings, the authors describe ways ethical analysis could take a more central role, and the developments creating momentum for it: AI-based health technologies, changes in the evidence landscape, assessing environmental impact, and the new EU HTA regulation. It is a reflection piece rather than a systematic review, but a useful signal of where HTA methods may be heading.

PMID: 41969054	PubMed →	DOI →
----------------	----------	-------

AI Research Paper 1

Development and pilot evaluation of a large language model-based clinical simulation system for medical education in gastroenterology.

Maimaris S, Tedino G, Memoli GA, et al. · BMC medical education · 2026

#ClinicalAI · #NLP

This pilot study built a system based on large language models that simulates whole gastroenterology consultations, from history-taking through to treatment and follow-up planning, so trainees can practise without real patients. Eight gastroenterology fellows (two initial testers and six blinded evaluators) rated the system across 160 evaluations on 20 cases, with mean scores of 4.32 to 4.57 out of 5 for realism, adaptability, accuracy and educational value. The authors describe it as an accessible and cost-effective tool for clinical reasoning training, though this is a small pilot.

PMID: 42351097	PubMed →	DOI →
----------------	----------	-------

AI Research Paper 2

Reporting completeness of clinical trials evaluating large language model interventions in medicine: systematic review.

Chen D, Blayne A, Ning T, et al. · BMJ (Clinical research ed.) · 2026

#ClinicalAI · #Regulation · #RealWorldEvidence

This systematic review searched for trial reports, protocols and registrations of large language model interventions in medicine up to December 2025, finding 68 trial reports, 15 protocols and 378 registrations. Reporting completeness was modest: trial reports met on average 40 to 59 per cent of the items in guidelines such as TRIPOD-LLM, CONSORT 2025, CONSORT-AI and CHART. LLM-specific details such as model versioning and inference parameters, and harms reporting, were inconsistently reported. For HEOR and regulatory teams it is a useful checklist of what evidence packages for LLM tools often lack.

PMID: 42869550	PubMed →	DOI →
----------------	----------	-------

This brief is produced using an AI-assisted workflow with expert human editorial review. Stories are curated and sources verified before publication. Readers are encouraged to consult source links directly.