

In the rapidly evolving landscape of digital health and regulated platforms, machine learning (ML) offers promising potential to detect and respond to behavioural risks early, guiding timely interventions. However, before deploying ML models on behaviour data—from patient portals to remote monitoring systems—practitioners must ground their approach in governance, evidence standards, and robust review processes. This article explores the foundational practical steps required before applying ML to behaviour data, drawing on examples from sectors such as healthcare, gaming regulation (e.g., MrQ), and research institutions like the National Institutes of Health (NIH).

Understanding Behavioural Risk as a Gradual, Pattern-Based Signal

One of the cardinal mistakes when working with behaviour data is treating individual events as standalone indicators. Behavioural risk seldom emerges instantaneously; rather, it appears gradually, embedded within patterns of digital interaction over time. For example, in healthcare remote monitoring systems, a single missed glucose measurement is less instructive than a sustained decline in daily readings or inconsistent reporting intervals. Similarly, gambling platforms like MrQ rely on behavioural signals aggregated over several sessions to flag potential problem gambling — single bets rarely tell the full story.

Recognizing this, the first practical step is to shift focus from isolated events to temporal patterns and trajectories:

- Collect longitudinal data that captures frequency, intensity, and variability of behaviours.
- Utilize analytics to identify recurring sequences or deviation from personal baselines.
- Involve domain expertise to define what meaningful patterns constitute risk.

These approaches ensure the ML models will reflect real-world behavioural dynamics rather than spurious correlations.

Governance First: The Pillar Before Data Use and Model Building

For regulated sectors—be it health or gambling—there is no shortcut around governance. “Governance first” means clearly establishing who owns the data, how it will be stored, shared, and most importantly, how decisions made from machine learning outputs will be overseen.

Healthcare examples abound, particularly in the management of patient portals and remote monitoring systems. The National Institutes of Health (NIH) emphasizes that any analysis involving patient behaviour must comply with strict privacy laws such as HIPAA and GDPR, along with ethical review board approvals. In parallel, regulated platforms like MrQ hold themselves accountable to gambling commissions, ensuring transparent and fair use of behavioural data.

Governance frameworks must address:

- **Data privacy and informed consent:** Patients and users must understand what data is collected and how machine learning will use it.
- **Data security:** Robust technical safeguards preventing unauthorized access.
- **Ethical oversight:** Multidisciplinary committees reviewing potential harms from algorithmic decisions.
- **Bias mitigation:** Ensuring models do not reinforce or amplify disparities.
- **Clear accountability channels:** Defining human roles in reviewing, challenging, and overriding model outputs where appropriate.

Evidence Standards: What True ‘Signals’ Look Like Versus ‘Stories’

A personal pet peeve—something I keep a running list of—is mixing “signals” with “stories.” Behaviour data is noisy, and it’s tempting to interpret spikes or drops as meaningful without sufficient evidence backing. Yet, sound evidence standards are the bedrock of trustworthy ML.



The National Institutes of Health’s research culture exemplifies rigorous evidence assessment by insisting on replicability, transparency, and clear operationalization of behavioural markers. This means:

- **Define clear operational criteria:** For example, what counts as “missed interaction” or “irregular use” in a patient portal?
- **Distinguish between correlation and causation:** Use statistical and experimental methods where possible to avoid misattribution.
- **Validate models with real-world outcomes:** Demonstrate that identified patterns predict important clinical or behavioural endpoints, not just data quirks.
- **Continual monitoring and updating:** Behavioural contexts evolve, and models require retraining to avoid degradation.

Practical example: A remote monitoring system might flag a patient as “non-compliant” due to reduced device usage. Instead of labeling this a failure, evidence standards ask: What would support look like here? Is reduced device use linked to improvement, device frustration, or new barriers like digital literacy issues? Without such inquiry, ML could penalize behaviour that is actually harmless or adaptive.

The Review Process: Human Oversight and Multidisciplinary Checks

No AI or ML system should operate in a vacuum—especially in sensitive behavioural domains. Before deploying machine learning on behaviour data, organizations must implement a multi-layered review process.

This includes:

- **Clinical/Domain expertise review:** Experts interpret whether flagged behavioural risk aligns with clinical knowledge or known social factors.
- **Ethics committee assessment:** Evaluating potential harms, benefits, and fairness.

- **Patient/User engagement:** Incorporating feedback loops where users can contest or contextualize machine-generated insights.
- **Regulatory compliance audits:** Ensuring ongoing alignment with local and international laws.
- **Algorithmic transparency:** Clear documentation of model logic, limitations, and confidence boundaries.

For example, at MrQ—a regulated gambling platform—any machine learning model that detects behaviour flagged as potential problem gambling must pass through review boards that include compliance officers, data scientists, and external regulators. Decisions around user interventions are never fully automated but involve a human-in-the-loop.

Summary: Stepwise Practical Guide to Starting ML on Behaviour Data

Bringing it all together, below is a stepwise practical approach before using machine learning on behaviour data:



1. **Establish governance framework:** Privacy, consent, accountability, and security must be foundational.
2. **Define what behavioural risk means:** Develop operational definitions based on expertise and evidence.
3. **Collect longitudinal, multimodal data:** Patient portals, remote monitoring systems, or regulated platforms like MrQ provide rich, temporal datasets.
4. **Build evidence-based models:** Validate behavioural signals against outcomes rather than focusing on single events.
5. **Implement multidisciplinary review processes:** Incorporate clinical, ethical, and regulatory oversight with human-in-the-loop checks.
6. **Plan for continuous monitoring and revalidation:** Behaviour evolves and so should models and governance.

Final Thoughts: Putting People and Privacy First

Technology enthusiasts often rush to ship AI features that promise insights from behavioural data. But without grounding in governance, evidence standards, and review, such efforts risk amplifying confusion, mistrust, and harm. As someone who's worked on remote monitoring rollouts and EHR alert governance committees, I've seen

[digital health analytics](#) firsthand how dashboards that celebrate clicks without explaining patient confusion miss the bigger picture.

Whether you're a digital health leader tapping into the National Institutes of Health's resources, a product manager at a gambling platform like MrQ, or a UX professional designing patient portals, remember: the first step is always "Governance First." Only then will your machine learning journey reflect responsible, human-centered innovation that respects privacy, embraces complexity, and ultimately improves outcomes.