COMMENTARY

Believing in black boxes: machine learning for healthcare does not need explainability to be evidence-based

Liam G. McCoya,*, Connor T.A. Brenna b,c, Stacy S. Chen c,d, Karina Vold e,f,g,h, Sunit Das g,i

a Temerty Faculty of Medicine, University of Toronto, Toronto, Ontario, Canada
b Department of Anesthesiology & Pain Medicine, University of Toronto, Toronto, Ontario, Canada
c Department of Philosophy, University of Toronto, Toronto, Ontario, Canada
d Joint Centre for Bioethics, University of Toronto, Toronto, Ontario, Canada
e Institute for the History and Philosophy of Science and Technology, University of Toronto, Toronto, Ontario, Canada
f Schwartz Reisman Institute for Technology and Society, University of Toronto, Toronto, Ontario, Canada
g Centre for Ethics, University of Toronto, Toronto, Ontario, Canada
h Leverhulme Centre for the Future of Intelligence, University of Cambridge, Cambridge, United Kingdom
i Division of Neurosurgery, University of Toronto, Toronto, Ontario, Canada

Accepted 1 November 2021; Available online 5 November 2021

Abstract

Objective: To examine the role of explainability in machine learning for healthcare (MLHC), and its necessity and significance with respect to effective and ethical MLHC application.

Study Design and Setting: This commentary engages with the growing and dynamic corpus of literature on the use of MLHC and artificial intelligence (AI) in medicine, which provide the context for a focused narrative review of arguments presented in favour of and opposition to explainability in MLHC.

Results: We find that concerns regarding explainability are not limited to MLHC, but rather extend to numerous well-validated treatment interventions as well as to human clinical judgment itself. We examine the role of evidence-based medicine in evaluating inexplicable treatments and technologies, and highlight the analogy between the concept of explainability in MLHC and the related concept of mechanistic reasoning in evidence-based medicine.

Conclusion: Ultimately, we conclude that the value of explainability in MLHC is not intrinsic, but is instead instrumental to achieving greater imperatives such as performance and trust. We caution against the uncompromising pursuit of explainability, and advocate instead for the development of robust empirical methods to successfully evaluate increasingly inexplicable algorithmic systems.

© 2021 Elsevier Inc. All rights reserved.

Keywords: Machine Learning; Explainability; Evidence-Based Medicine; Mechanistic Reasoning; Algorithms; Artificial Intelligence

1. Introduction

The incredible growth of the machine learning for healthcare (MLHC) field has spurred both optimism and concern in the medical community. Proponents are drawn to the prospect of rapid algorithmic analysis of patient data on a massive scale enabling cheaper, more efficient, and more accurate medical care. Purposed uses include both those which overlap with physician expertise (such as reading CT scans with similar accuracy to a radiologist [1]), and those which will extend beyond it (such as performing analyses of voice waveform data to predict the onset of dementia [2]). A number of machine learning techniques central to this recent progress, such as “deep learning”, involve the analysis of large amounts of data to generate outputs based on highly complex sets of and interactions between data features [3]. Such techniques have been characterized as “black boxes” [4] as they can perform with a high degree of empirical accuracy while being unable to indicate to human observers specifically why and how a specific output has been attained.

This “black box” inexplicability has led to significant disquiet amongst critics of MLHC – broadly divided into the categories of performance-related (e.g., inexplicable MLHC may be ineffective, or may be unable to adapt

Conflict of interest: Dr. Sunit Das declares roles as: Advisory board for Subcortical Surgery Group and Xpan Medical, Consultant for Medexus, Speaker’s Bureau for Congress of Neurological Surgeons, American Association of Neurological Surgery, Society for NeuroOncology. Grant funding from CIHR, Medicienna, Alkermes. Clinical trialist for Agios. The other authors declare no potential conflicts of interest.

* Corresponding author.

https://doi.org/10.1016/j.jclinepi.2021.11.001
0895-4356/© 2021 Elsevier Inc. All rights reserved.
What is new?

Key findings:

- Explainability is instrumental to important aims in machine learning for healthcare (MLHC), but a closer analysis in its full context reveals that explainability cannot be considered intrinsically essential to MLHC.
- What this adds to what is known?
  - This work explores the connection between explainability in MLHC and its analogue of mechanistic reasoning in evidence-based medicine.
- What is the implication, what should change now?
  - MLHC should not be held to a unique standard of explainability beyond that required of other medical interventions.
  - Established tools used to validate evidence-based medicine should be adapted to enable empirical evaluation of even completely inexplicable MLHC technologies.

2. The desire for explainability in MLHC

Proponents of explainability argue that systemic opacity will interfere with the ability of human oversight to identify and address errors arising from naive misinterpretation of data without contextual clinical understanding [7,10]. A prototypical example of this is an MLHC model which erroneously identified asthma as a protective factor against pneumonia severity, when in reality the “protective effect” was a manifestation of the aggressive use of intensive care for asthmatic patients [17]. Similar concerns arise regarding the inability of models to properly identify and highlight findings which are rare but highly consequential, such as an aggressive subtype of lung cancer on radiographic imaging [18]. In light of these failures, explainable MLHC may be expected to facilitate a sort of partnership between the physician and the algorithm, with human oversight preventing errors and inaccuracies.

The pursuit of explainability can, however, exert cost on performance. Extracting information from models which may have millions of parameters and presenting this information in a way understandable to the human mind is an inherently reductive process [19]. Trade-offs may arise between accuracy and explainability [20,21], as reducing opacity may motivate the use of more simplistic models, or the evaluation of smaller and more comprehensible pools of data. However, MLHC models are valued precisely because they have the potential to process information in ways—and at speeds—that are impossible for human brains to match. Even if such insight is achieved, relying upon human oversight into the algorithmic prediction system raises a broad new range of human factors challenges [22]. Explainability is therefore not costless, and from the perspective of MLHC performance it must be viewed as one among several means rather than an ultimate end in itself.

There are also significant concerns surrounding the ability of inexplicable models to fulfill the ethical duties of medicine and achieve the trust of patients and providers; informed by the sense that the frameworks established for artificial intelligence (AI) should echo the principles and standards to which physicians are held [23]. Guidelines for ethical production and the use of artificial intelligence systems, such as the one published by the European Commission, require AI to uphold principles of explica-
bility, prevention of harm, fairness, and human autonomy [24]. These overarching requirements parallel the *prima facie* principles of medical practice and biomedical ethics: beneficence, non-maleficence, justice, and autonomy [25].

From this perspective, it becomes clear that the desire for explainability in AI parallels the desire for transparency from human physicians. The expectation in both cases is that the patient will be provided with adequate and coherent information needed to make informed choices which result in predictable and ideal outcomes [26]. From the provider perspective, clinicians have identified explainability as an important element of transparency, and a requisite to justify their reliance upon a given MLHC model [27]—particularly in the context of informed consent [28], legal liability concerns, and a lack of regulatory clarity [29].

Patients and providers alike seek the assurance that an MLHC algorithm is making appropriate recommendations, and explainability provides a way to better understand, engage with, or control MLHC. Nonetheless, we propose that it is difficult to argue that an interest in explainability is intrinsically morally valuable, let alone foundational to ethical acceptance of a new technology given that trust in predecessor technologies in healthcare has been established through empirical means, typically without the clarity of understanding mechanisms. Just as in the case of performance, explainability is an instrumental means of establishing and maintaining trust and control, but is not a critical end in and of itself.

3. The reality of (Un)explainability in healthcare

In discussions around the need for explainability in MLHC, such as Char and colleagues’ declaration that “ML systems in medicine must have an explainable architecture, designed to align with human cognitive decision-making processes” [7], there is irony in recognizing that these human cognitive processes themselves often escape explainability [20,30–32]. One sees this empirically in the finding that, in contrast with the rules-based approaches of beginners, the inferences of expert radiologists tend to be so holistic that their underlying reasoning cannot be explained in natural language [33,34]. What are presented as ‘explanations’ in such cases may in fact be post-hoc rationalizations. Indeed, it has been argued that every diagnosis is, to some degree, a “clinical diagnosis”—relying on subtleties of clinical judgment which extend beyond a clearly explainable or rules-based framework [35].

Beyond the cognitive domain, inexplicability is also pervasive in the various tools at the clinician’s disposal. From acetaminophen [36] to metformin [37], or many antidepressants and mood stabilizers [38], numerous medications are prescribed regularly—and to great effect—despite the fact that their mechanisms of action are partially or even entirely unclear. Even certain surgical procedures, such as gastric bypass for obesity [39–41], are performed despite their mechanisms of action not being fully understood. This lack of explainability does not, however, diminish the utility of such therapies.

Ultimately, the primary goals of medicine are pragmatic: to relieve suffering and promote health [6]. The elucidation of mechanisms comes secondary to this goal, insofar as understanding may enable better intervention, may support informed consent, or may provide greater comfort to patients and families. Some have, in fact, contested the very concept of explainability in medicine: for this reason, explainability lacks a consensus definition within the medical context [42]. Instead, modern medicine has constructed a scientific edifice to evaluate the pragmatic impact of interventions whose mechanisms are not fully understood [43]—the robust infrastructure of EBM, which privileges outcomes as its measure of success.

4. Empirically validating the inexplicable

The history of tools used in medical practice which have resisted mechanistic explanation reaches its apotheosis in the paradigm of EBM which, in exploring the epistemological tensions surrounding these longstanding therapies, has already precipitated the development of a relevant concept: mechanistic reasoning. Mechanistic reasoning refers to the inferential use of a proposed process of action to rationalize the expectation of a given outcome, which is broadly analogous to the role invoked for explainability in the MLHC context [44] (though indeed it is worth noting that, in both contexts, this reasoning is often performed *a posteriori* working backwards from an observed result).

At its core, EBM revolves around using the best available evidence (e.g., randomized controlled trials rather than anecdotes), in combination with individual clinical expertise and patient values, to guide decision-making [45–47]. However, discourse surrounding the role of mechanistic reasoning in EBM has not yet reached consensus [44,48]. Traditionally, mechanistic reasoning has been considered lesser than correlative or statistical reasoning in hierarchies of evidence [48,49]. This view is supported by the unpredictable nature of human physiology—biological mechanisms tend to have high complexity, and a probabilistic disposition which challenges mechanistic reasoning [44]. Consequently, mechanistic explanations can lead to false conclusions, and mechanistic reasoning alone has been shown to have a high degree of fallibility. At times empirical results can be entirely contrary to mechanistic expectations, as in the case of prophylactic antiarrhythmic drugs actually acting to increase mortality from arrhythmia after recurrent acute myocardial infarction [50]. Mechanistic reasoning is not, therefore, sufficient to guide evidence-based practice.

Plausible mechanistic suggestions are critical in the development of new hypotheses [51], and may be useful in extrapolating the results of a statistical finding to a new population [52,53]. Biological plausibility features as one of nine Bradford Hill criteria for defending any suggestion of causality (although with the explicit caveat that it is
wholly dependent on contemporaneous biological knowledge, and therefore not always available) [54]. Biological plausibility has also gathered traction in more recent interpretations of causality like the Russo-Williamson Thesis, which suggests that causality in the health sciences requires both mechanistic and probabilistic (or “difference-making”) evidence, and that the former can complement the latter [55,56]. Mechanistic reasoning does have demonstrable utility as a form of evidence, but considering EBM’s progress in its absence, we argue that such reasoning cannot be considered strictly necessary for evidence-based practice.

At its core, the issue of explicable in MLHC becomes a question about appropriate rationale: what type and amount of evidence is compelling enough for the implementation of a new intervention in clinical practice? In the case of mood stabilizers, effective interventions with undetermined mechanisms were embraced rather than discarded—empiricism was used to circumvent the demand for mechanistic reasoning. In other words, clinicians and policy makers effectively chose to tolerate mechanistic uncertainty in exchange for well-evidenced utility. Rigorous clinical testing is able to validate such interventions, characterizing their full range of positive and negative effects in the absence of any knowledge of their mechanisms. Thus, clinical practice under the EBM framework is privileged towards statistically sound evidence that an intervention does work, even in the absence of mechanistic evidence as to why it would.

Similarly, the benefits and consequences of MLHC can be discovered and validated consequentially, through robust empirical analysis of even its most inexplicable outputs. Empirical evidence is also relevant to the various ethical dimensions in which a need for explainability in MLHC has been invoked. With fairness, for example, the relevant dimension is the performance of the algorithm for different groups, which depends on the (empirically visible) outputs of the model, rather than any underlying reasoning. Indeed, prominent case studies have demonstrated precisely how explainable (and not intentionally biased) models can nonetheless deliver biased results that are only apparent upon empirical analysis [57,58]. Similarly, the trust of both patients and physicians might be established through empirical evaluation and regulatory approval similar to that of any pharmaceutical or other medical technology.

It is important to highlight that awareness of the potential costs of explainability, however, does not imply that inexplicable models are superior in all cases. Indeed, in certain medical contexts (such as predicting heart failure outcomes from claims data) explainable logistic regression models have demonstrated similar efficacy when compared to more complex MLHC systems [59]. Small disparities may not be clinically meaningful, and in certain contexts explainability may be considered worthwhile in exchange for a small degree of reduced performance [60]. Further, significant work is being done toward the development of methods to improve the explainability of complex methods, offering a hope of “opening the black box” and enabling presently inscrutable deep learning architectures to become explainable [61–63]. As with other healthcare interventions whose mechanisms were better clarified over time, increasing explainability may arise in parallel with or subsequent to the implementation of black-box models through evidence-based evaluation.

There are specific and valid reasons for concern regarding the challenges of empirically validating MLHC tools, such as concerns that shifts in the underlying population may render a model inaccurate over time [64], or concerns that a continuously updating model may develop aberrant characteristics. These concerns can and should drive the adaptation of rigorous empirical methods to the specific needs of the MLHC context. Yet as with numerous other tools used in medicine, from pharmaceuticals to clinical reasoning aids to the very cognition of clinicians, the utility of MLHC is largely independent of our ability to fully explain its actions. Explainability has its value in this context, but to regard it as essential for effective and ethical MLHC is to apply a unique burden of proof to this particular class of emerging technology and to underestimate the capabilities of well-validated EBM concepts to be adapted to succeed in this novel context.

5. Conclusion

In examining the reasons that explainability tends to be a desirable feature of contemporary MLHC, we observe that these reasons are instrumental rather than intrinsic. Explainability is sought as a means toward ensuring model effectiveness and developing trust in both patients and providers. While explainability in MLHC may indeed advance these interests, an examination of other domains reveals that the scientific community has robust and well-established mechanisms for evaluating the effectiveness of (and developing trust in) tools that are not mechanistically explained or explainable. It must not be forgotten that significant trade-offs may arise between explainability and other interests, such as accuracy and overall performance. To narrowly emphasize the importance of explainability for the use of a medical tool would be to reject not only certain types of MLHC tools but also the well-validated and trusted edifice of EBM.

Continued work must be done to explore the trade-offs inherent in the pursuit of explainability in MLHC in any given domain. Tensions are likely to arise between raw predictive performance and the abstractive simplification necessary for an algorithm to be explainable, particularly in the bedside context. Achieving an optimal balance will depend on the specifics of the clinical context, and the strength of the validation procedures in place. Ultimately, however, we must not forget that artificially intelligent tools are attractive precisely because they are able to perform tasks of data synthesis and analysis at a scale and
speed not achievable by human cognition. In limiting machines to reasoning as humans do, we may rob them—and ourselves—of their unique potential to solve problems which we cannot.

**Final Contributions Statement**

*Liam G. McCoy: Conceptualization, Investigation, Writing - Original Draft, Writing - Review & Editing. Connor T. A. Brenna: Conceptualization, Investigation, Writing - Original Draft, Writing - Review & Editing. Stacy S. Chen: Conceptualization, Investigation, Writing - Original Draft, Writing - Review & Editing. Karina Voldz: Conceptualization, Writing - Review & Editing. Sunit Das: Conceptualization, Writing - Review & Editing, Supervision

**References**


