Information Fusion as an Integrative Cross-Cutting Enabler to achieve Robust, Explainable, and Trustworthy Medical Artificial Intelligence

Andreas Holzinger\textsuperscript{a,b,*}, Matthias Dehmer\textsuperscript{c,d}, Frank Emmert-Streib\textsuperscript{e}, Natalia Díaz-Rodríguez\textsuperscript{f}, Rita Cucchiara\textsuperscript{g}, Isabelle Augenstein\textsuperscript{i}, Javier Del Ser\textsuperscript{n,o}, Wojciech Samek\textsuperscript{p}, Igor Jurisica\textsuperscript{j,k,l,m}

\textsuperscript{a}Medical University Graz, Austria
\textsuperscript{b}Alberta Machine Intelligence Institute, University of Alberta, Canada
\textsuperscript{c}University of Medical Informatics Tyrol, Austria
\textsuperscript{d}Swiss Distance University of Applied Sciences, Switzerland
\textsuperscript{e}Predictive Society and Data Analytics Lab, Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland
(Andalusian Research Institute in Data Science and Computational Intelligence (DaSCI Institute). University of Granada, Spain.
\textsuperscript{f}University of Modena and Reggio Emilia, Modena, Italy
\textsuperscript{g}Artificial Intelligence Research and Innovation Center, Modena, Italy
\textsuperscript{h}Department of Computer Science, University of Copenhagen, Copenhagen, Denmark
\textsuperscript{i}Osteoarthritis Research Program, Division of Orthopedic Surgery, Schroeder Arthritis Institute, University Health Network, Toronto, Canada
\textsuperscript{j}Krembil Research Institute, Data Science Discovery Centre for Chronic Diseases, University Health Network, Toronto, Canada
\textsuperscript{k}Departments of Medical Biophysics and Computer Science, University of Toronto, Canada
\textsuperscript{l}Institute of Neuroimmunology, Slovak Academy of Sciences, Bratislava, Slovakia
\textsuperscript{m}TECNALIA, Basque Research and Technology Alliance (BRTA), Derio, Spain
\textsuperscript{n}University of the Basque Country (UPV/EHU), Bilbao, Spain
\textsuperscript{o}Departments of Artificial Intelligence, Fraunhofer Heinrich Hertz Institute, Germany

\section*{Abstract}
Medical artificial intelligence (AI) systems have been remarkably successful, even outperforming human performance at certain tasks. There is no doubt that AI is important to improve human health in many ways and will disrupt various medical workflows in the future. Using AI to solve problems in medicine beyond the lab, in routine environments, we need to do more than to just improve the performance of existing AI methods. Robust AI solutions must be able to cope with imprecision, missing and incorrect information, and explain both the result and the process of how it was obtained to a medical expert.

\textsuperscript{*}Corresponding author
Email address: andreas.holzinger@medunigraz.at (Andreas Holzinger)

Preprint submitted to Information Fusion May 31, 2022
Using conceptual knowledge as a guiding model of reality can help to develop more robust, explainable, and less biased machine learning models that can ideally learn from less data. Achieving these goals will require an orchestrated effort that combines three complementary Frontier Research Areas: (1) Complex Networks and their Inference, (2) Graph causal models and counterfactuals, and (3) Verification and Explainability methods. The goal of this paper is to describe these three areas from a unified view and to motivate how information fusion in a comprehensive and integrative manner can not only help bring these three areas together, but also have a transformative role by bridging the gap between research and practical applications in the context of future trustworthy medical AI. This makes it imperative to include ethical and legal aspects as a cross-cutting discipline, because all future solutions must not only be ethically responsible, but also legally compliant.

**Keywords:** Artificial Intelligence, Information Fusion, Medical AI, Explainable AI, Robustness, Explainability, Trust, Graph-Based Machine Learning, Neural-Symbolic Learning and Reasoning

---

### Graphical Abstract

Figure 1: Graphical abstract: Information Fusion as integrative cross-sectional topic
1. Introduction and Motivation

Artificial intelligence in medicine is on everyone’s lips. Politicians around the world have declared it a desired goal. Industry sees it as an enormous growth engine and medicine envisions it as a great opportunity for medical problem solving and decision support. AI and machine learning will, and are already transforming many biomedical problems and associated clinical workflows. As a result, the society has lately witnessed an upsurge of stories and use cases where medical AI-based models have taken a capital role in realizing unprecedented levels of diagnostic performance [1, 2, 3, 4, 5, 6, 7, 8, 9].

The substrate for growing medical AI-based systems in the near future has expanded even further after the saddening 177 million COVID-19 cases and 3.85 million deaths held globally as of June 17th, 2021. On the positive side, we deal with unprecedented health-related data – in volume, veracity, diversity and uncertainty. Due to variation across countries with respect to false positives and false negatives of performed tests, testing frequency and reporting frequency and quality, these data have unknown uncertainties. In addition, there are many unknowns that are not systematically recorded, including lifestyle, compliance with recommendations and misinforming data sources. Any interpretation and conclusion drawn from data in the medical domain should consider these challenges. However, it is clear that due to large numbers, trends provide useful insights, suggesting that despite similar economies, health care systems, and population densities, some countries rank better than others when considering cases per million and deaths per million (see Figure 2). Certainly, quality and number of tests are critical, and can either increase or decrease confidence on these trends.

Indeed, the broader data availability has brought about the renewed interest in AI algorithms for the medical domain, particularly convolution neural networks in image analysis, and specifically in radiology and pathology. However,
to use AI to solve problems in medicine and life sciences beyond the laboratory and in routine settings, there is an urgent need to go beyond simple benchmarking and improving the performance of methods that only operate on independent and identically distributed (i.i.d.) data. Unfortunately, even the best current machine learning models do not generalize well, have difficulty with small training datasets [10], and are sensitive to even small perturbations [11] [12] [13].

Above all, AI-based models are difficult to impossible for human experts to interpret and, most importantly, unable to infer causal relationships therefrom. Robustness and explainability have been declared by the European Union as the definitive most important properties for future successful medical AI [14]. Additionally, robustness and explainability are important prerequisites for discovering causal relationships and providing explanations based on them, thus enabling the verifiability of machine decisions by a human expert in a given context. This cannot be achieved by a single approach, but requires concerted action from complementary fields. In medicine, different modalities (image, text, omics) [9] [15] may contribute to an outcome, hence hindering the provision of
actionable explanations and robustness guarantees.

A fundamental claim to be elaborated in this work is that information fusion can serve as a means to facilitate re-traceability, explainability and interpretability in these difficult contexts [16]. A primary challenge is to combine, fuse, and process high-quality data with partial information, to extract knowledge, and to make the underlying explanatory factors interpretable – that is, to make them traceable, comprehensible and verifiable to the medical expert – on demand. On demand means that not everything and all has to be explained immediately and constantly just in time, but that, on request, a human expert has to be able to understand how a result achieved by algorithms came about. This is due to legal requirements: the General Data Protection Regulation (GDPR) establishes transparency as a key principle along with lawfulness and fairness, both of which are important parts of accountability. The GDPR has caused an extensive debate of this so-called “right to explanation” in legal academia (e.g. [17, 18, 19, 20, 21, 22]) and the impact has also been felt in Computer Science [23]. This argues for the “Prohibition of decisions based solely on automated processing” in order to avoid considering individuals as inhuman ‘subjects’ in an automated decision-making process determined solely by machines, as this would lead to the loss of human autonomy, thus to the loss of human control and responsibility [24]. That means that a final decision should always be made with the human-in-control.

Moreover, a common representation is necessary, especially to make unknown relationships in lower dimensions accessible to the human expert. Contributions in this direction will have a major impact on AI in general and machine learning in particular. Novel tools are needed to understand relationships and make machine decisions transparent and reproducible. This traceability and verifiability will ultimately increase confidence in future AI methods. One possibility is to use a human-in-the-loop approach [25, 26, 27], as human experts are able to contribute contextual understanding and implicit domain knowledge that can complement current statistical, data-driven learning methods. However, this cannot be done by a simple combination, but requires radically
novel approaches. Consequently, future medical systems in particular will re-
quire the design, development, and evaluation of mathematical frameworks for
structural causal models \cite{28,29} that involve, for example, the use of typed
graphs to formalize cause-effect relationships. These graphs need to be anno-
tated with diverse relationships between e.g. genes, non-coding RNAs, proteins,
and metabolites through curated interaction data, providing the mechanism for
causal models. Such approaches require new human-AI interfaces where domain
experts can interactively create queries and simulations of possible counterfac-
tuals, for example, to answer “what if?” questions \cite{30}.

Future AI should be as robust as natural human intelligence is. One way to
achieve this is to incorporate prior human knowledge \cite{31} and ensure that an
AI-based system can inherently evolve over time in an efficient human-machine
symbiosis. Contextual knowledge can thereby be introduced into the machine
learning pipeline, integrated into the explanation method, or derived from ex-
planations \cite{32}.

Research and teaching are trying to keep up with AI trends aimed at ad-
dressing these functional needs for medical AI. However, in most cases advances
reported in specialized fora cannot meet expectations with the growing demands.
A systematic preparation of the topic of medical AI in research and teaching is
not only necessary, but crucial for the practical and effective implementation of
AI in the future to ensure the increasing demand for highly qualified special-
ists. The task of this new generation of experts will be to bring the latest AI
research developments into the day-to-day applications to ultimately deliver on
the promise that AI will be used for the benefit of all people.

The goal of this position paper is to identify the most relevant pioneering
frontier research areas and make the case for why and how they can contribute
to a concerted integrative effort to make future medical AI efficient and effective
in practice. Specifically, we discuss on three Frontier Research Areas (FRA):

1. Complex Networks and their Inference (CNI);

2. Graph Causal models and Counterfactuals (GCC); and
(3) Verification and Explainability Methods (VEM).

All through the above FRA, we advocate for information fusion as the integrative cross-cutting catalyst that unleashes a great chance to unify and synergize these three FRA. The new "AI summer" is causing an exponential increase not only in interest in AI, but also an actual increase in the use of AI in all areas of life, including medicine. This inevitably raises questions of reliability, safety, fairness, as well as moral and ethical integrity [33], in addition to questions of robustness and explainability. Therefore, ethical and legal aspects must always be included. All future solutions must not only be ethically responsible [34], but also legally compliant [35]. The European Union has taken a clear stance on AI: AI must be human-centered and trustworthy. To be trustworthy, any AI must comply with applicable rules and regulations, adhere to ethical principles, and be implemented in a secure and robust manner, as defined by the EU High-Level Expert Group on AI [2].

To this end, and following the schematic diagram shown in Figure 1, a cyclic, iterative, agile human-centered AI redesign process, based on agile user-centered design methods [36] is needed to intertwine the proposed frontier topics with respect to the proposed information fusion approach, eventually reaching the degrees of trustworthiness, robustness and explainability required to fully harness the potential of medical AI.

This paper is organized as follows: for each Frontier Research Area, we begin with a few selected specific problems to show what problems each FRA addresses. We proceed by describing why the topic under study by every FRA is a problem for medical AI, and the extent to which the current state of the art falls short of what is needed to solve the problem. We then describe how the problem can be addressed, and present some promising work in the literature that goes in the right direction for this FRA. In a subsequent section, which we refer to as "Desiderata", we list some general characteristics and features

that future technical achievements in this FRA should have for this application domain. We conclude each section by highlighting the practical benefits of realizing this FRA and how it will help bridge the gap between scientific achievements and their practical implementation in the medical domain. Of course, our postulations and thoughts offered for each FRA only scratch the surface, and are therefore far from complete. However, our firm intention is to raise awareness among the international research community, policy makers, and stakeholders to focus efforts on these promising cutting-edge topics for the benefit of better and more efficient medicine for all.

2. Frontier Research Area 1: Complex Networks and their Inference

2.1. What: Fighting complex diseases poses many problems in the integration and scalability of machine learning methods

Exploring and researching complex diseases such as arthritis, brain disorders, cancer, or infectious diseases such as COVID-19 requires novel medical decision support systems that are able to incorporate not only humans into the loop, but also integrative analyses combining diverse omics datasets along with clinical information from a wide variety of modalities [37], using scalable methods for data fusion and mining [38], machine learning, statistics, graph theory and graph visualization into low-dimensional representations because human cognition is not optimized to work well in high-dimensional spaces . Among the myriads of properties describing genome, epigenome, transcriptome, microbiome, phenotype, lifestyle, etc., no single data type, however, can capture the complexity of all the factors relevant to understanding a phenomenon such as a disease. A key challenge is the identification of effective models to provide a relevant systems view [39].

Additional insights can be gained and in vivo validations better planned by trying to understand the conservation of deregulated genes, networks, and pathways across organisms [40] [41] – which is a major and, to date, unsolved problem.
Developing effective knowledge repositories to support the governance, processing, inference, analysis and interactive visualization of integrated omics [9] and network data is essential [42]- [56]. Integrating diverse assays and algorithms, in turn, helps to address both false positives and false negatives [57] [58].

2.2. Why: Integrating data with networks makes it possible to identify novel relationships between data silos

Currently, explainable AI (XAI) developments are mostly uni-modal. However, enriched, more feasible explanations in the medical domain can be achieved if they consider multimodality. Integrating data with networks – protein interactions networks, transcription regulatory networks, microRNA-gene networks [59], metabolic and signaling pathways – enables to identify relationship among data silos [60]. Further analyzing these annotated networks with graph theory algorithms or knowledge engineering tools provides insights into their structure [61] [62], which in turn, can characterize the function of these proteins, transcription factors and microRNAs [63]. Combining machine learning, data mining and graph theory is difficult, but critical to maximize the impact on translational research [64], enable more accurate and explainable modeling, increase our understanding of complex diseases [65] [66] and, ultimately, support P4 medicine (precision, personalized, participatory, preventive) medicine [67] [68] [69].

Challenges at the intersection of machine learning and network biology for Next-Generation Machine Learning for Biological Networks, which could impact disease biology, drug discovery, microbiome research, and synthetic biology are discussed in Camacho et al. (2018) [70].

2.3. How: Quantitative graph theory can help interpret integrated omics data within diseases

Graphs have been used in life sciences for a long time. In recent years, there is a growing trend to combine elements of graph theory, machine learning, and statistical data analysis, which offers tremendous opportunities especially to support interactive knowledge discovery for personalized medicine [71]. In
network analysis, complex biomedical graph data is examined, and the increasingly easy generation of large amounts of genomics, proteomics, metabolomics etc., and signaling data enables the construction of large networks that provide a framework for understanding the molecular basis of physiological and pathological conditions. Such complex networks have been investigated extensively for several purposes [72, 73]. On the one hand, networks have been explored in the context of studying complex systems by means of graphs. Examples thereof are biological, linguistic, chemical and technical networks [74]. Other contributions in this area relate to study motifs and modules within complex networks [73]. On the other hand, lots of quantitative analyses on networks have been performed [75].

To shed light on this problem, we briefly sketch Quantitative Graph Theory, introduced by Dehmer and Emmert-Streib [76]. Quantitative Graph Theory can be divided into two major categories, namely Comparative Network Analysis, Network Characterization and networks explainable by design. Comparative Network Analysis relates to measuring the structural similarity between networks [77]. This can be done by using so-called exact or inexact graph matching, see [78, 79]. Exact graph matching is based on the concept of graph isomorphism. Inexact graph matching relates to determining a gradual change on the similarity between graphs by utilizing graph invariants. Another approach for measuring the similarity between graphs is based on utilizing topological indices as an input when using distance or similarity measures for real numbers [80].

Next, Network Characterization using quantitative graph complexity measures can be employed. A network measure is a function that maps network instances to positive real numbers. In mathematical chemistry, they are often referred to as topological indices [81]. Many complexity measures for graphs have been developed, e.g., based on distances, vertex degrees, graph automorphism and so forth. We refer to [82, 83] for more details. One promising domain for the future is the emerging field of geometric deep learning, which is an umbrella term for new techniques that attempt to generalize (structured) deep neural models to non-Euclidean domains, such as graphs and manifolds.
Machine learning of networks is promising and has recently been used very successfully to fight Covid-19 [85].

With respect to networks explainable by design, compositional part-based object detecting and classifying neural symbolic explainable models [25] can aid the explanations based on not only on coarse grained labels, but more fine grained findings, and provide a wider provenance that traces the explanation to the very source, i.e., at the data acquisition stage. This goes beyond current XAI techniques that limit their explanations to provide rationale only for a given input and output sample data [86, 87, 88]. Going beyond uni-modal explanations makes the information fusion aspect to be of paramount importance in the explanation process, to allow traceability from the data collection, to the output explanation interfaces with a diverse set of audience profiles that participate in the medical and clinical processes characterized by different backgrounds and expertise.

Apart from the methods sketched above, networks have also been used in other areas including data mining, machine learning, lexical semantics, information fusion [89, 90, 91, 92] and integrative computational biology, such as cell differentiation [62].

Despite inherent noise present in interaction datasets, systematic analyses of these networks uncover biologically relevant information, such as lethality [93, 94], functional organization [95, 96, 97, 98], hierarchical structure [62, 99, 100], modularity [63, 101, 102] and network-building motifs [61, 103, 104], even across time [68]. This suggests that networks have a strong structure-function relationship [61], which can be used to help interpret integrated omics data within diseases [107, 60], across diseases [108] and across organisms [55, 54], understand drug mechanism of action and toxicity [109], and performing causal inference on big data [15].
2.4. Desiderata: Fusing machine learning with systematic graph theory promotes the knowledge gain of multi-modal data and their interrelationships

Many interactions are transient, so networks change in different tissues or under different stimuli [55, 110, 111, 112]. Studying the dynamics of these networks is an exponentially complex task. Many stable complexes show strong co-expression of corresponding genes, whereas transient complexes lack this support [113, 114]. These contextual network dynamics must be considered when linking interactions to phenotypes and when studying the networks topology. Analyzing such insights on the network dynamics towards the identification and minimization of different biases of individual detection methods, the simple intersection of results achieves high precision at the cost of low recall.

Systematic graph theory analyses of dynamic changes in interaction networks, combined with probabilistic modeling [115], and integrated with gene and protein cancer profiles enable comprehensive analyses of complex diseases such as cancer [116, 117, 118], generating new insights [69, 60], robust biomarkers [107, 108, 119] and models that explain causal relationships through network inference [120, 121]. Implementing algorithms using heuristics fine-tuned for interaction networks [122, 123, 124] will ensure their scalability. Finally, we also highlight achievements reported lately on the use of Deep Learning methods to undertake modeling problems formulated over interaction networks, which have so far elicited promising results [125, 7].

2.5. What for: Pushing the boundaries in this FRA will help understanding complex diseases

There are many benefits emerging from early steps taken along this FRA. For instance, some of the most successful network-based methods of gene group identification for class prediction have been the score-based sub-network markers [126, 127, 128, 129]. Sub-networks identified using these approaches were recently shown to be highly conserved across studies and to perform better than individual genes or pre-defined gene groups at predicting breast cancer metastasis [127]. Improving these methods by considering network modularity results
in better prediction of aging \cite{63}. Combining existing known and predicted interactions with novel local co-expression annotation of existing edges will elucidate disease-specific dynamics and identify local network structures (graphlets, \cite{123,130}) that are the most aberrant components in the cancer network, as compared to a normal control case. Network dynamics \cite{110}, in turn, enable explainable modeling of healthy and disease signaling cascades \cite{131}, or modeling cancer progression \cite{68}.

3. Frontier Research Area 2: Graph Causal Models and Counterfactuals

3.1. What: Causal learning from observational data is a central problem relevant to many application domains

Causal learning from pure observational data and predictive modelling is a general problem relevant for many application domains. It is gaining much interest recently and has been largely tackled by the AI community \cite{132,133}. There are a number of fundamental problems that have existed for a long time and have not yet been solved. The renowned American philosopher Charles S. Peirce argued that human induction must be guided by special aptitudes for guessing right, which led to the challenge of simplicity or parsimony, which is even going back to Occam’s razor. Alone, the concept of simplicity poses a lot of problems for both causal machine learning \cite{134} and causal human learning \cite{135}. If causal inference has a rational basis, we would expect the resulting causal knowledge to allow the formulation of coherent answers to a variety of causal questions.

Two main problems about causal relationships can be distinguished in the literature: (1) “What is the probability that a cause causes (or prevents) an effect?” and (2) “What is the probability that a causal relationship exists between these two variables?” Or, put another way, “Does the cause have a nonzero probability of producing (or preventing) the effect?” \cite{136}. The generality and wide spectrum of practical scenarios in which such questions can be formulated makes
the discovery of causal relationships from data a subject under vibrant study in diverse fields and disciplines. AI-based medicine is not an exception, with specific tasks such as diagnosis and treatment calling for further advances in causality inference that unveil novel interventional and prescriptive strategies from medical data.

3.2. Why: Typically, the underlying causal model that accounts for all factors affecting an outcome variable of interest is missing

A common challenge in applying causal analysis is the lack of an underlying causal model that can account for all factors influencing an outcome variable of interest. Recent progress has been done on causal signal extraction from images \cite{137,138}. Causality has also been applied to generative neural networks and proxy variables in an attempt to better deal with the kind of data used by Deep Learning \cite{139,140}. Nevertheless, the international research community agrees that there are a lot of shortcomings and many open problems to be solved, for instance, dealing with the all possible underlying, and often unknown, factors of variation and variables on which causality is feasible to be studied in practice \cite{141,133,142}.

3.3. How: XAI with counterfactual explanations and causal algorithmic recourse can help determine what is causally related

Formal reasoning about causal relations between features \(X = [X_1, \ldots, X_d]\) can be done by using a structural causal model, i.e. a non-parametric model with independent errors according to Judea Pearl \cite{143,144}. In the following we introduce some basics to show how this can be helpful. For more extensive introductions, please refer to \cite{136,145}. The data-generating process of \(X\) is described by an (unknown) underlying structural causal model \(\mathcal{M}\) of the general form:

\[
\mathcal{M} = (\mathbf{S}, P_U), \quad \mathbf{S} = [X_r := f_r(X_{pa(r)}, U_r)]_{r=1}^{d}, \quad P_U = P_{U_1} \times \ldots \times P_{U_d}. \quad (1)
\]

The structural equations \(\mathbf{S}\) are a set of assignments generating each observed variable \(X_r\) as a deterministic function \(f_r\) of its causal parents \(X_{pa(r)} \subseteq X \setminus X_r\).
and an unobserved noise variable $U_r$. Here it is important to note that $P_U$ is a factorising joint distribution over background variables which introduces uncertainty due to the lack of observations. The assumption of mutually independent noises (i.e., a fully factorised $P_U$) entails that there is no hidden confounding and is referred to as causal sufficiency. For an experimental proof, we refer to Karimi et al. (2020) [145].

Structural causal models are often represented by a so-called causal graph $G$. Such causal graphs can be obtained by drawing a directed edge from each node in $X_{\text{pa}(r)}$ to $X_r$ for $r \in \{1, \ldots, d\}$.

Figure 3b and Figure 3c show a typical textbook example. We assume henceforth that $G$ is acyclic. In this case, the data-generating process $M$ implies a unique observational distribution $P_X$, which factorises over $G$, defined as the push-forward of $P_U$ via $S$.

The structural causal model framework allows for the study of interventional distributions, describing a situation in which some variables are manipulated externally. The structural causal model also implies distributions over counterfactuals, i.e. statements about (hypothetical) interventions that were all else being equal (Ceteris Paribus, namely, the analysis of the effect of one variable on another, assuming that all other variables remain the same).

When formulated in the context of classification via a model $h$, a popular approach to the study of counterfactuals is to find so-called (nearest) counterfactual explanations [18] where the term “counterfactual” is meant in the sense of the closest possible “fact” with a different outcome. Counterfactual predictions consist of asking ourselves what would have been the effect of something if we had not taken an action, i.e., alternative scenarios [14], or modifications of the input data that could eventually alter the original prediction of the model $h$, and help the user understand the performance boundaries of the model for improved trust and informed criticism. Interventional clinical predictive models require the calculation of counterfactuals, apart from the correct specification of cause and effect [14]. Just to give an example, to analyze counterfactuals based on the structural causal model $M$, an intervention (also known as do operator)
can be used to indicate that a set of variables \( X' \subseteq X \) is fixed to \( \gamma \), which is often denoted as \( do(X' = \gamma) \). The corresponding distribution of the remaining variables \( X \setminus X' \) can be computed from \( \mathcal{M} \) by replacing the structural equations for \( X' \in S \) to obtain the new set of equations \( S(do(X' = \gamma)) \). The interventional distribution \( P_{X'|do(X' = \gamma)} \) is then given by the observational distribution implied by the manipulated structural causal model \( (S_{do(X' = \gamma)}, P_U) \).

\[
S = \begin{cases} 
  X_1 := f_1(U_1), \\
  X_2 := f_2(X_1, U_2), \\
  X_3 := f_3(X_1, X_2, U_3)
\end{cases}
\]

\[P_U = P_{U_1} \times P_{U_2} \times P_{U_3}\]

(a) Classifier-centric view of a factor graph. (b) Causal model \( \mathcal{M} = (S, P_U) \). (c) Causal graph \( \mathcal{G} \) for \( \mathcal{M} \).

Figure 3: Counterfactual explanations (a) treat features as independently manipulable inputs to a given fixed and deterministic classifier \( h : \mathcal{X} \to \{1, \ldots, L\} \) trained to make decisions about i.i.d. samples from the data distribution \( P_X \). In the causal approach to algorithmic recourse taken in this work, we instead view variables as causally related to each other through a structural causal model \( \mathcal{M} \) (in (b)) with associated causal graph \( \mathcal{G} \) (c) [145].

Given observations \( x_{obs} \), the definition of the \( do(\cdot) \) interventional operator permits, for example, to ask what would have happened if \( X' \) had instead taken the value \( \gamma \).

An answer to this question departs from the definition of the counterfactual variable by \( X(do(X' = \gamma))|x_{obs} \), and the distribution of this counterfactual variable can be computed in three steps [144]:

1. **Abduction**: first compute the posterior distribution over background variables given \( x_{obs} \), \( P_U|x_{obs} \).

2. **Action**: perform the intervention to obtain the new structural equations \( S_{do(X' = \gamma)} \); and
3. Prediction: then compute the counterfactual distribution $P_X(\text{do}(X' = \gamma)|x_{\text{obs}})$
induced by the resulting structural causal model $S^{\text{do}(X' = \gamma)}, P_U|x_{\text{obs}}$.

Causal inference and counterfactual prediction for actionable healthcare are discussed in Prosperi et al. (2020) [146]. In medical applications, some of the tests for measuring robustness of estimated effects on non pharmaceutical interventions include intervention models doing different structural assumptions and validation of such assumptions when they do not hold. An example of such interventions against COVID-19 includes generalization over countries presented in [147]. In cases where causal effect estimation is aimed at individual-level recommendations, alerting decision makers when predictions are not to be trusted is crucial. Therefore, identifying failure with uncertainty-aware models (e.g., when covariate shift makes training and test datasets vary), as proposed in [148], facilitates uncertainty communication to decision-makers. Generally, uncertainty enables deep learning methods to be adopted into clinical workflows [149].

A different but intuitively similar concept related to the characterization of counterfactuals is that of contrastive explanation [150], which consists of explaining not only why an event occurred, but also why it occurred as opposed to some alternative event. They are considered necessary for agents to achieve moral responsibility, although a debate exists on contrastive explanations entailing causal determinism [151, 152]. Approaches producing contrastive explanations serve to learn more efficiently from data. For example, using pertinent negatives [153] is one among such approaches, and relates to learning structural descriptions from examples. Another example is using active learning, which can help select the most informative pairs of labels to elicit contrastive natural language explanations from experts, while dynamically changing the model [154].

Equally important is the integration of “Big Data” methods with explanations that involve a causal analysis. This integrated analysis is key, especially in omics and imaging for causal inference [155]. An example of such tight in-
tegration is the use of deep feature selection for causal analysis in Alzheimer’s Disease \cite{155}. Other example is the alignment of domain expert knowledge with Deep Learning models in order to achieve more expert-compatible explainability. Neural-symbolic learning and reasoning systems can be used for this purpose with different kinds of integration schemes \cite{156,25}.

3.4. Desiderata: Disentangling influential factors from multivariate observations and plausible yet diverse counterfactuals

A concern with causal AI in medicine is how to disentangle correlated factors of influence in high-dimensional settings. One way to deal with the independent manipulation of as set of correlated factors is to disentangle the influence of correlated factors from multivariate observations with interventions. An example of such is Back-to-Back regression \cite{157}, to help identifying the causal contributions of co-linear factors in multi-variate and multi-dimensional magnetic resonance imaging observations. Back-to-Back regression produces an interpretable scalar estimate for each factor from a set of correlated factors to estimate those that most plausibly account for multidimensional observations. As a result, this method disentangles respective contributions of collinear factors to identify the causal contribution of covarying factors.

In regards to counterfactual explanations, the plausibility, feasibility, and diversity of the obtained counterfactual explanations (whether they are contrastive or not) are particularly relevant aspects that should be considered in the medical domain. In this regard we advocate for an increasing prevalence of modern generative learning approaches applied to the discovery of counterfactuals. The capability of such methods to model the distribution of existing multi-dimensional data yields a proxy generator of plausible hypothesis that can be of utmost help to ensure that counterfactual instances can occur in reality. Further along this line, the diversity of counterfactuals can be a conflicting objective with their plausibility as per $P_X$, hence counterfactual generation methods should also properly balance among such objectives \cite{158}.
3.5. What for: Causality and counterfactual generation may reduce diagnostic results, increase quality of care and life, reduce overall costs, and free up clinicians’ time

As in other fields with strong human interaction, in designing a medical AI system it is critical to consider who will use it. Furthermore, when the system is used for diagnostics, it is also crucial to ensure proper balance between sensitivity and specificity, and to optimize the user interface and workflow integration. There are numerous examples that support these claims from pathology, radiology and dermatology, e.g. a smartphone based melanoma classifier would likely be used by general public as a first step in screening for skin diseases.

Here the main goal – specially when the treatment for the disease to be diagnosed is invasive or has serious side effects for the health of the patient – is to maintain a low false negative rate. On the other hand, a system for radiologists should automatically classify common cases, and leave the decision on more complex cases for the expert, aiming at a high true positive rate. Properly using such systems would reduce false negatives and false positives, increase quality of treatments and quality of life of patients, decrease the overall cost and free-up clinicians’ time, which becomes more critical as decision-making situations become more patient-centered [159].

Advances on graph causal modelling and counterfactuals can be a major step towards realizing such objectives. On one hand, interventional clinical studies can be driven by the results of causal analysis of multi-dimensional medical data, thereby eliciting new diagnostic and treatment criteria that in turn, produces data from such new cases that can be fed back to the AI-based models. On the other hand, counterfactuals can increase the trustworthiness of the medical expert on the decisions issued by the AI model, discerning when it must not be fully relied as a result of a counterfactual being close to the case to be diagnosed/treated. This augmented information offered to the expert could reduce the amount of false positives, thereby favoring the aforementioned decrease of costs and efforts.
4. Frontier Research Area 3: Verification and Explainability Methods

4.1. What: The use of AI requires the ability to verify correctness and causal accuracy

In the medical domain, the use of AI and machine learning models that are explainable and verifiable by human medical experts is an absolute necessity, primarily for legal reasons [160]. The central problem is that no AI method will be deployed if its results cannot pass a verification process for correctness and causal accuracy by a human expert on demand. Making these assessments is difficult if the AI methods in question do not provide explanations to users. The problem becomes clear when we consider the classic problem described by Caruana et al. (2015) [161], where an AI system trained to predict a person’s risk of pneumonia came to incorrect conclusions, and applying this model would have increased, not reduced, the number of patient deaths. At the same time, this is also a good example of the usefulness of having a human-in-the-loop, because physicians can easily verify the results based on their experience – namely, that such results of an AI system are not correct after all. Moreover, a human in-the-loop approach can bring in contextual understanding, implicit knowledge and experience to statistical machine learning methods, and consequently provide prior knowledge. However, one core open problem remains, namely, how to integrate this knowledge into the machine learning pipeline.

The term verification comes from both software engineering and medicine and was used in AI as well [162], the term explainability is used to technically highlight decision-relevant parts of machine representations, i.e., parts that contributed to the accuracy of a particular prediction. However, such a technical explanation does not refer to a human model. For this, explainability must be extended to include the concept of causability [163], which refers to a human model. Causability was introduced in reference to the well-known term of usability [164]. While explainability is about implementing transparency and traceability, causability is about measuring the quality of explanations, i.e., the measurable extent to which an explanation of a statement achieves a certain
level of causal understanding for a user with effectiveness, efficiency, and satisfaction in a given context of use [165]. In other words, causality measures whether an explanation achieves a given level of causal understanding for a human. This is a major challenge in the medical field, as many different modalities contribute to a single outcome, requiring multimodal causality [37].

4.2. Why: The best machine learning methods to date lack robustness and are difficult to interpret

Currently, the most important and most lacking aspect of AI in general, and in medical AI in particular, is robustness. Recent success in machine learning has led to an explosion of AI applications, resulting in high expectations being placed in autonomous systems, such as autonomous vehicles [166, 167], medical diagnosis [168, 169], industrial prognosis [170], or cybersecurity [171]. These developments require that we recognize and understand the fundamental limitations of current intelligent systems, which often apply across many different application areas. This crucial deficit of robustness of current systems concretely relates to their lack of ability to adapt to changes in the environment. In medicine, this is even more profound, as data changes because of changes in patient cohorts, due to advancements of instruments and assays that generate images and omics data, and as a result of changes of treatment modalities and our understanding of health and disease states at physiological and molecular levels.

The field of machine learning deals with the development of successful adaptation strategies and attempts to enable machines to recognize or respond to changing conditions for which they have not been specifically programmed or trained. So far, however, most work in machine learning has been based on the “independent identically distributed” assumption. That is, the machine must be able to process new input data that have not been seen during training, but that they conform to the same statistical distribution. As the i.i.d. assumption is a strong assumption that is rarely met in practice, the field of machine learning is currently working extensively on theoretical and empirical approaches to
develop learning strategies that do not require this assumption to hold. These efforts are particularly related to the concepts of “transfer learning” \[172, 173\], “domain adaptation” \[174, 175, 176\], “adversarial training” \[177, 178, 179, 180\] and “lifelong” or “continual learning” \[181, 182\].

Even if non-i.i.d. issues are circumvented or simply do not occur, an obstacle to reach fully actionable medical AI is the lack of explainability. In particular, modern Deep Learning models that nowadays monopolize modeling approaches for medical imaging usually remain “black-boxes” \[86, 183, 184\] that are unable to explain the reasons for their predictions or recommendations. This property largely precludes the diagnosis and correction of defects, and only favors conservative safety assessments of the behavior of a learning model. Both problems are very much related to a lack of understanding of cause-effect relationships. This hallmark of human cognition is a necessary (though not sufficient) component for machine learning methods achieving human-like intelligence, which would provide the basis for a much broader application of AI in industry and business. A grand issue in the task of learning from a set of observed samples is to estimate the generalization error of learning algorithms. The problem with these typical measurements, e.g., the training error, is that they are biased, particularly if the available amount of data is small. Traditionally this is measured by complexity measures such as the Vapnik-Chervonenkis (VC) dimension \[185, 186\], or stability \[187\].

In the race towards properly characterizing and understanding medical AI-based models, one cannot ignore the importance of providing important features for explainable models, which becomes particularly essential for image processing algorithms \[155\]. Furthermore, these systems need to be integrated with existing research and clinical workflows. Importantly, proper independent verification and explainability methods may highlight that well-performing AI systems are reportedly superior to humans in some clinical systems (or e.g., radiologist-level \[188\]), and unveil the reasons why their outperforming behavior can degrade severely in other healthcare systems as a result of potentially non-identically distributed data resulting from a context-induced bias \[180\].
4.3. How: Causal approaches and explainability methods can contribute to achieving target trials, transportability, and predictive invariance

From the previous section it is clear that robustness is a key aspect to be addressed in medical AI-based systems. Performance guarantees can only be given if models are proven to be robust against different phenomena that compromise their generalization capability. An interesting approach to study generalization of learning algorithms from the perspective of robustness was presented in [190], which derived generalization bounds for learning algorithms based on their algorithmic robustness. The assumption is that if a testing sample is “similar” to a training sample, then the testing error is close to the training error, which is different from the traditional complexity or stability arguments mentioned earlier that concentrate on solely optimizing pure performance measurements.

Indeed, in the machine learning community the overall trending goal seems to be maximizing standard accuracy, and many papers from the biomedical domain report increasing accuracy levels for different medical diagnostic tasks by virtue of models of increasing complexity and sophistication. However, such models still yield erroneous cases, which should motivate doctors to retrace and find the rooting cause of such errors. However, a non-automated inspection and verification of such cases is often unfeasible due to the multi-modality of data and the efforts it requires from the medical expert. At this point a new opportunity arises for causality and explainability as enablers to automate this medical verification process.

Unfortunately, observational biomedical studies are affected by confounding and selection biases among other biases [191], which makes causal inference infeasible unless robust assumptions are made. These require a priori domain knowledge, as data-driven predictive models can be used to infer causal effects. However, neither their parameters nor their predictions necessarily have a causal interpretation.

Consequently, we firmly call for the use of causal approaches and learning causal structures by using certain linchpins to develop and test intervention models [146], namely: 1) target trials, 2) transportability, and 3) prediction in-
variance. To begin with, target trials refer to algorithmic emulation of randomized studies. Transportability [192] is a license to “transfer causal effects learned in experimental studies to a new population, in which only observational studies can be conducted”. Akin to transportability is prediction invariance, where a “true causal model is contained in all prediction models whose accuracy does not vary across different settings”. When a causal structure is available or a target trial design can be devised, the evaluation of model transportability for a given set of action queries (e.g., treatment options or risk modifiers) is recommended; while for exploratory analyses where causal structures are to be discovered, prediction invariance could be used. In this way, as advocated by Prosperi et al. (2020) [146], transportability and prediction invariance could become guideline core tools and part of reporting protocols for intervention models, for a better alignment with the standards for prognostic and diagnostic models of medicine and biomedical practice today.

Another phenomenon placing at risk the trustworthiness and verification of medical AI models is their robustness to adversarial attacks. Technically, we assume a model processing unseen examples from the underlying distribution $P_X$. In general, the goal of model training is to reach a minimum of a expected loss function [193]. However, many machine learning models, particularly deep neural networks [194], are susceptible to be deceived by the presence of adversarial examples [195]. Adversarial examples can be conceived as modified data instances resulting from small yet intelligently tailored perturbations made to original examples. Even if they are not even visible to the human eye, such perturbations yield dramatic effects when processed through the machine learning model, provoking a wrong output with high confidence.

Figure 4 depicts a schematic diagram showing the different reasons by which model verification and robustness assessment are of utmost necessity in the medical domain. XAI methods can help determining what a model observes in an input when predicting its output, ascertaining the presence of biases inherited from data or purposely inserted by adversarial attacks. Likewise, counterfactual explanations can also benefit for stronger input-output causal relationships
Tests to guarantee Robustness

1) Adversarial attacks (maliciously purposed perturbations)
2) Counterfactual explanations (plausible what-if hypothesis)
3) Inherently biased inputs (predictive artifacts inherited from data)

Figure 4: Schematic diagram exemplifying the different circumstances under which robustness of a medical AI-based systems (in this case, for diagnosing a melanoma) must be verified: adversarial attacks, counterfactual explanations and biases. Causality inference and explainability methods can enable automated means to perform such a verification procedure.

discovered from data, stepping beyond the production of correlation-based counterfactuals to the generation of interventional what-if stories. This might be a major step in the medical AI field to trascend from verifiable models for diagnosis towards verifiable AI-based solutions for medical prescription and treatment.

A pause must be done before proceeding further to highlight, once again, the importance of having a human-in-the-loop as the ultimate stakeholder to decide whether an AI-based model is robust enough [27]. Even if the verification process can be partly automated by XAI and causality inference methods, trustworthiness always requires a qualitative assessment of the overall verification process, both in terms of their starting assumptions (e.g. is a certain adversarial attack strategy for a medical AI-based model plausible and likely to occur in the context in which data are produced?) and the results it conveys (corr. is the detected bias inherited from data? Can we reduce this bias by preprocessing or improving the data collection process anyhow?). All in all, humans, even if we make mistakes, can be considered a robust proxy in decision making when informed with quantitative and well-summarized measures of algorithmic robustness.
4.4. Desiderata: Adversarial training can contribute to better robustness and explainability

A very different use of adversarial training is to make models more robust and interpretable. The work in [196] shows that adversarial training improves the interpretability of gradient-based saliency maps in medical imaging diagnosis of skin cancer. In particular, adversarially trained convolutional neural networks are significantly sharper and more visually coherent than non-adversarial traditionally trained CNNs. What many of these robustness tests highlight is the needs for verification and validation methods for deep learning techniques beyond academic toy datasets. It is clear that much of the research efforts have focused on overfitting deep learning models with ever-increasing numbers of parameters to a small selection of research benchmark datasets [197].

Even results reported in carefully curated international challenges such as PASCAL VOC [198] later turned out to be largely based on spurious correlations (e.g., ships were classified by the presence of water, or horses were linked to copyright watermarks). In a similar vein, popular text classification datasets have been shown to contain biases, meaning that only parts of the input are needed to make the correct predictions [199]. This type of cheating is also referred to as “Clever Hans effect” [200].

In spite of permitting the incremental improvement and incredible advances in the field, natural image datasets can normally be very different from real life datasets, which are more sparse, noisy and in uncontrolled settings. Language differences aside, similar conclusions can be derived from medical text data collected in diverse environments, which ground on cultural, geographical or individually-induced biases present in such data. Generalizing to real life datasets is thus a part of the desiderata of having robust machine learning models for medical application. For this to occur, we envision that explainability tools will become increasingly relevant, becoming a core part of prospective studies reporting successful real-world cases.
4.5. What for: The most important practical benefit of implementing this FRA theme is maintaining trust

In the medical domain, the use of AI methods that are verifiable, comprehensible and interpretable by human experts will not only be mandatory for legal reasons in the future, but also offers a number of other technical and non-technical advantages. Advantages from the technical point of view include that developers get a better understanding of the medical system endowed with AI-based functionalities, thus are able to improve existing methods (e.g., by reducing complexity or model size) with increased knowledge about the niches and directions along which such improvements can be attained. Bias identification [201] or adversarial attack detection [202] can be arguably the most evident examples of technical advantages granted by XAI methods for model verification.

Above all, the big advantage for the medical expert and the end user affected by decisions issued by verified medical AI models lies in the increased trust on their outcomes, the remaining responsibility of the human being (human-in-control) and the avoidance of bias and discrimination. Medical decisions can pose a turning point in the life of a patient, so trustworthiness on the suitability of decisions issued by such models is a must at many different levels of the medical workflow, from the diagnosis (confidence of predictions), to the design of the treatment (suitability of prescribed therapies/medication by a model) and the acceptability of the patient (causability to ensure that he/she understand that the AI-informed decisions are the best ones for his/her disease). When understanding this need for trustworthiness at multiple levels of the medical workflow, one can realize the enormous relevance of AI verification and explainability in the medical realm.
5. A Unified View on the Integrative Role of Information Fusion in Medical AI

Encoding multidimensional data, but also tabular data and data of temporal sequential nature, is an open challenge for the latest DL models to assimilate incomplete and irregular healthcare data. Reinforcement learning and explainable models to fully control this family of AI black-box models [203] can better use this data for sequential decision making from observational multi-modal data if meaningful representations are learned and used to represent a patient state [204].

In this context, local and global explanations are equally important, i.e., assessing machine learning model output with respect to a single input data point, also called “decision understanding” (e.g., as done by methods such as Local Interpretable Model-Agnostic Explanations - LIME [205] or Layer-wise Relevance Propagation - LRP [206]), but also verifying and certifying the full model at a global scale, also called “model understanding” [207]. Likewise, [208] advocates for explanations in cooperative decision making in medicine to be mutual, implicitly implying a continual fusion of explanations. Mutual explanations [209] are introduced in a context of transparent expert companions towards medical decision support systems where interactive and explainable HRI [210] machine learning plays a key role. Mutual explanations naturally provide the understanding of verbal explanations, i.e., based on dialog incremental processes to provide human machine learning users with trust and deeper involvement in the learning process. When explanations are not accepted, the human cannot only ask for them but also correct them. This way, expert domain knowledge is used in learning and inference through explanation sketches that are applied as constraints for the inductive logic programming system Aleph.

Verbal interpretability perspective [211] is achieved by ensuring that the model is capable of providing humanly understandable statements, e.g., logical relations, showing positive words drawing to a conclusion, verbal chunks or sentences [212] that indicate causality, and that the model produces explanations...
which are non-contradictory, non-redundant, fluent and cover all important aspects related to the prediction [213].

Also related to human expert alignment are the needs for developing models for clinical acceptance. An example of such good practice is shown in [214], where such acceptance test is done through ratings by ophthalmologists on the correlation of the attribution method scores with diagnostic features. In this context, in addition to local explainable models of a single sample, approaches to test global explanations such as TCAV (Testing with Concept Activation Vector) [215] or SpRAy (Spectral Relevance Analysis) [200] are desired in order to explain beyond a single data point example. However, they may not be fully considered as global method, as they only consider the set of all training examples from a given class [211]. Another critique of current Natural Language Processing (NLP) models provided with verbal interpretability is the lack of provision of the actual underlying mechanisms to generate texts. Generating free text explanations is often framed as a summarization task – either as extractive settings, where salient sentences from provided evidence documents are selected as explanations [213], or abstractive settings, where, given evidence documents, the explanation is produced from scratch using a generative model [210]. While the latter can result in more fluent explanations and incorporate further background knowledge not explicitly present in the evidence documents, it is known that, as for example used for EHR generation from conversations in [217], fake facts are hallucinated by neural generators [218]. Yet other works rely on hybrid approaches, where extractive summarization is followed by abstractive summarization [219, 220]. However, as also advocated by [211], further work on providing explanations of the process and shape of the embedding optimization is needed.

The role of natural language in information fusion and XAI is two-fold: on the one hand, language is one of the data modalities, in which complex facts and relationships are expressed, e.g. in electronic health records (EHRs) or medical literature. On the other hand, language is the prime channel of explanation: verbalizing the algorithmic reasoning enables the health practitioner to easily
detect whether the reason for the algorithmic decision is acceptable.

For both variants, the use of cross-modal representations that link, e.g., textual, image and omics data will be crucial for AI in multimodal data as present widely in the medical domain. Challenges lie in the harmonization and curation of cross-modal datasets aligned across two or more modalities enabling the cross-modal transfer, either by learning a common subspace via methods such as DCCA \[221\] or by projection learning \[222\]. While suitable datasets are becoming available in the public domain, they are yet to be constructed for medical data.

For processing and generating language in a transparent way, future work will have to concentrate on NLP models with provenance, i.e., models that provide the data on which their output is based on. In the case of automatic summarization, for example, this would be the statements that lead to the formulation of a summarizing sentence; for semantic processing it could be the use of hybrid models that combine sparse representations \[91\] with dense representations, e.g., \[223\]. For Transformer-based architectures (e.g., \[172\]), in the absence of human rationales to train a model to generate explanations, this could be realized with attention scores, although they only loosely correspond to human-acceptable explanations \[224, 13, 225\]. An alternative could be to investigate the utility of diagnostic properties, such as Faithfulness, Dataset Consistency and Confidence Indication \[88\]. These have been shown to be useful for automatically evaluating the quality of explanations, and might be suitable as objectives for generating explanations in an unsupervised way. Another option is the use of (intransparent) NLP technologies to identify and extract information with provenance, as for example done in \[226\] for metadata extraction from biomedical literature to increase reproducibility of studies.

Metrics worth assessing beyond model understanding through subspace explanation (MUSE) induce fidelity (based on instances disagreement between model and explanation), unambiguity (in terms of rule overlap and cover), or interpretability (in terms of triple rule set size, width, and predicate size) \[227\].

One strand of future methods strives for high quality data in order to pro-
duce better predictions, the requirements to deploy AI systems in medicine advocate as well for natural handling of noisy and incomplete data, which is much more realistic in healthcare, where many information silos due to the distributed nature of domain expert knowledge bases and respective EHR. In this line, techniques to complete partial data from missing sensor readings through data level- and feature level information fusion to improve the overall data quality include, for instance, kernel random forests in fog computing for heart disease prediction [228]. Another example showing improved results with extra fused data includes the use of self-attention architectures for CT-image and non visual features for immunotherapy treatment response prediction [229]. In fog computing, a similar approach to federated learning in terms of data decentralization, the ability to access all data at once is not possible. However, fusing the different sensors available for different users makes all data actionable [146], and the full set richer, and of better quality. Recent work showed that it is even possible to train largely personalized models in such distributed settings [230].

Other strand of ideology advocates for approaches that incorporate a natural handling for anomalies and outliers [231], as well as incomplete, dirty and irregular datasets, as a common feature of medical AI systems [232]. The latter work also warns for the potentially large impact of unintended consequences of machine learning in medicine from an empirical and technical viewpoint. These and other pitfalls in data-driven decision making [146] are to be considered in the development of the frontier topics discussed in this paper, hand in hand with experts-in-the-loop.

Integrative computational biology and AI algorithms play a central role in precision medicine. Individual analyses can be combined using multiple networks, including transcription regulatory, microRNA-gene, physical protein interactions, metabolic and signaling pathways [233]. Such analyses help identify better prognostic and predictive signatures, drug mechanism of action, combination therapies, and possible novel drug targets. These networks can be further annotated with tissues and diseases to form richly-annotated typed graphs, which in turn can be analyzed with graph theory algorithms to form explainable
models. For example, Bhattacharyya and colleagues integrated a pathway-based patient model with multi-scale Bayesian network to predict specific treatment options [23]. Similarly, exploring the possible links between AKT1 (Akt is a Protein kinase B that plays a key role in glucose metabolism, apoptosis, cell proliferation, transcription and cell migration) and BTK (Bruton’s tyrosine kinase that plays a crucial role in B cell development and signaling), we obtain 1,862 proteins connected by 2,324 edges (i.e., direct physical protein interactions, 437 uni-directional, 84 bi-directional and the rest non-directional), as shown in Figure 5. The network in this figure highlights which of the interactions are relevant to arthritis, neuro-degenerative diseases, or cognitive disorders.

Figure 5: Exploring the connection between AKT1 and BTK. The physical protein interaction network from the Integrated Interactions Database (IID v.2020-05) [55] highlights the Gene Ontology biological process (node color) and disease annotation from DisGeNET (edge color); specifically, arthritis, neurodegenerative diseases, cognitive disorders, and their overlap (thicker, darker color edges).

Importantly, once a hypothesis and model are created from an integrative analysis, such as the one highlighted in Figure 5, one would need to select the most appropriate – and ideally, the least costly – organism to act as the model for further functional studies and validation. Considering this network, the
mouse would be the best model organism, as about 98% of all interactions in the network are conserved from human to mouse, while the rabbit has only 33% of the network conserved, and fly, worm and yeast have none of these interactions present (Figure 5 a). Using analogous selection, the most relevant tissues for functional validation include adipose, lung, spleen and bone (81%-85%), falling to just around 50% for heart and brain (Figure 5 b). Considering diseases, only cancer has a substantial set of annotated interactions in this network with almost 60% of the network being annotated to diverse cancers (Figure 5 c).

Figure 6: Conservation of the physical protein interaction network from Figure 5 across a) non-human species, b) tissues, and c) diseases.

As we have seen in previous sections, for AI models in medicine, there are several concerns with respect to the development of these frontier topics. Besides them, another dimension with large concerns in medicine whose importance can be exacerbated upon the fusion of multimodal data is the privacy and confidentiality awareness of medical AI-based models. Indeed, the compliance with patient privacy normally hinders medical AI methods from excelling in practical settings due to a diversity of reasons, such as the increased difficulty of collecting data, restrictions to their use following ethical and legal constraints, or the potential performance penalty obtained when data are encoded prior to modeling. Ideas using the concept of differential privacy [235], privacy-preserving representations [236] or along the lines of privacy distillation [237] are key to further develop this line of work. Privacy distillation [238] allows patients to decide the type and amount of information they disclose to healthcare information systems.
while retaining the model accuracy under a sufficient subset of original privacy-relevant features. The idea behind this model-agnostic mechanism is to balance accuracy of the model with the redacted inputs of users. An example of application in a DL regression setting for dose prediction is in [238]. It demonstrates to reduce the amount of over-prescriptions and under-prescriptions of warfarin. To sum up, we foresee that the growing amount and diversity of patient, medical and clinical information combined and flowing together into medical processes relying on AI-based models will give rise to unprecedented challenges in what relates to the privacy of sensitive data, calling for overarching strategies that maintain the confidentiality of protected information of the patient all over the process.

6. Conclusion

In this position paper we have identified and outlined three crucial Frontier Research Areas to develop within AI and biomedicine, hand in hand. These frontier topics are worthwhile investing and would dramatically benefit from a Frontier Development Lab. For example the SETI-NASA-ESA FDL programme for AI + Space + Earth Sciences showcases an exemplar very successful implementation [239] that benefits from a catalyzing environment for tackling some of the most challenging interdisciplinary research problems [240]. Putting together, in similar synergy, future biomedical AI would benefit from cross-domains research teams to solve challenges within multi-science problems.

This also requires additional doctoral schools in this domain that follow such a research-based approach. Experts at the interface between AI/machine learning and biomedical/life sciences are urgently needed worldwide. For example, in the European Union there is already a dramatic shortage on skilled AI experts generally; industry is desperately looking for suitably trained specialists and the risk of losing the competitive edge is huge [241]. Besides reproducibility, robustness and explainability discussed above, biomedical AI applications need to consider confidentiality, ethics and legal aspects, and how and by whom AI
will be used. This requires that future experts also need to be taught ethical and legal aspects cross-sectional, not only theoretically, but they also need to be given the opportunity to put this into practice in health facilities and industry, which calls for new agile human-centered AI design methodologies.

Ignoring the implications of improper usability planning may lead to incorrect results and reduced applicability. This requires one to weigh up sensitivity with specificity to ensure specialist vs general use cases or screening vs treatment planning. It is also important to ensure clear understanding of limitations based on validation – which patient cohorts may or may not be appropriate for a given trained model. Besides explicitly acknowledging and recognizing the limitations of these AI models and resulting systems, patient-centric medicine requires models to provide specific confidence and uncertainty estimates on the recommendation for each patient, rather than simply provide broad accuracy measures across cohorts.

One size does not fit all. While AI can solve standard cases with similar accuracy to human experts, it cannot yet beat human specialists. However, we rather stand with the synergy that flourishes when AI and the specialist collaborate together, feeding each other with knowledge that allow them performing better, more robustly and reliably in their respective tasks. Human-in-the-loop systems would benefit from AI approaches, and even more from an ensemble of AI systems, implemented using different approaches and algorithms, and trained and validated on different patient cohorts. Conversely, AI-based systems can leverage the qualitative verification of the knowledge captured from data, as well as the conformity of explanations with the medical expertise and the evidence recorded over the medical workflow.

To realize this holistic vision, it is important that ongoing studies dealing with medical AI are verified swiftly, providing informed evidence that AI-based models for medical practice can be trusted. On the other side of the coin, research retractions should be managed and resolved quickly, as done in recent COVID-19 related research contributions (e.g., Mehra et al. (2020) in *The New England Journal of Medicine* and *Lancet*, Mulvey et al. (2020) in *35*
However, the process takes a long time – mistakes are usually detected and retracted within months, but fraud often takes years [245]. This has direct, negative implication for evidence-based medicine, and a significant impact on computational biology and AI. Considering requirements for training and validation of AI systems, data from retracted papers may affect large number of workflows and analyses, leading to incorrect models and interpretations. Training or validating AI systems on flawed data may not be obvious immediately, and even when the paper is retracted, data will likely exist in multiple forms on the Web for years after.

To circumvent this latter issue, online data repositories are crucial, but stringent curation processes are essential to ensure high quality, reliable and properly annotated data. For example, the IMEx consortium [42, 246, 43, 247, 248] curates interaction data from published literature to enable integrative computational biology analyses, and ensure the implementation of data-driven medicine and the correct analysis and interpretation of model results. The availability of such curated repositories, and evidences of real-world AI-based models that largely rely on advances over the frontier topics reviewed in this position paper would free-up specialists by solving straightforward cases automatically, and comprehensively characterizing complex cases for further consideration and inspection.

In this holistic vision of medical AI, we highlight the cohesive role of information fusion as a technology to transport all medical data modalities through the frontier research areas. New challenges around multi-modal explanations, causality (cause–effect) and causability (quality of explanations) analysis are still to be addressed by the research community for achieving full trustworthy and robust medical AI-based systems and the use of new types of human-AI interfaces and supportive visualizations. The element of visualization plays an important role here, because it is ultimately what is presented to the expert end user [249]. The insights and knowledge from the long established field of visual
analytics must therefore be comprehensively considered and integrated into new future overall solutions.

We hope that this position paper, as a reference for research and research-based teaching, will establish some directions to be pursued in the coming years to realize the vision of human-centered AI.

Acknowledgements

Andreas Holzinger acknowledges funding support from the Austrian Science Fund (FWF), Project: P-32554 explainable Artificial Intelligence; Natalia Díaz-Rodríguez is supported by the Spanish Government Juan de la Cierva Incorporación contract (IJC2019-039152-I); Isabelle Augenstein’s research is partially funded by a DFF Sapere Aude research leader grant; Javier Del Ser acknowledges funding support from the Basque Government through the ELKARTEK program (3KIA project, KK-2020/00049) and the consolidated research group MATHMODE (ref. T1294-19); Wojciech Samek acknowledges funding support from the European Union’s Horizon 2020 research and innovation program under grant agreement No. 965221 (iToBoS), and the German Federal Ministry of Education and Research (ref. 01IS18025A, ref. 01IS18037I and ref. 0310L0207C); Igor Jurisica acknowledges funding support from Ontario Research Fund (RDI 34876), Natural Sciences Research Council (NSERC 203475), CIHR Research Grant (93579), Canada Foundation for Innovation (CFI 29272, 225404, 33536), IBM, Ian Lawson van Toch Fund, the Schroeder Arthritis Institute via the Toronto General and Western Hospital Foundation.

References


[17] P. Goodman, S. Flaxman, European Union Regulations on Algorithmic


[40] B. Cox, M. Kotlyar, A. I. Evangelou, V. Ignatenko, A. Ignatenko,


URL http://dx.doi.org/10.1038/ng.2764


URL https://doi.org/10.1145/3236386.3241340


54


[167] K. Muhammad, A. Ullah, J. Lloret, J. Del Ser, V. H. C. de Albuquerque,


URL https://www.aclweb.org/anthology/P07-1033

URL https://www.aclweb.org/anthology/W06-1615


URL https://www.aclweb.org/anthology/2020.nlpmc-1.4


URL https://www.aclweb.org/anthology/N19-1357


URL http://knowledge.amia.org/65881-amia-1.3897810/t003-1.3901461/f003-1.3901462/2731669-1.3901539/2731984-1.3901536


