

---

# ARTIFICIAL INTELLIGENCE-DRIVEN CLINICAL DECISION SUPPORT SYSTEMS

---

A PREPRINT

**Muhammet Alkan**

School of Computing Science  
University of Glasgow  
Glasgow, Scotland, UK

**Idris Zakariyya**

School of Computing Science  
University of Glasgow  
Glasgow, Scotland, UK

**Samuel Leighton**

School of Health and Well Being  
University of Glasgow  
Glasgow, Scotland, UK

**Kaushik Bhargav Sivangi**

School of Computing Science  
University of Glasgow  
Glasgow, Scotland, UK

**Christos Anagnostopoulos**

School of Computing Science  
University of Glasgow  
Glasgow, Scotland, UK

**Fani Deligianni\***

School of Computing Science  
University of Glasgow  
Glasgow, Scotland, UK  
[Fani.Deligianni@glasgow.ac.uk](mailto:Fani.Deligianni@glasgow.ac.uk)

February 18, 2025

“The advance of technology is based on making it fit in so that you don’t really even notice it, so it’s part of everyday life.” — Bill Gates

## ABSTRACT

As artificial intelligence (AI) becomes increasingly embedded in healthcare delivery, this chapter explores the critical aspects of developing reliable and ethical Clinical Decision Support Systems (CDSS). Beginning with the fundamental transition from traditional statistical models to sophisticated machine learning approaches, this work examines rigorous validation strategies and performance assessment methods, including the crucial role of model calibration and decision curve analysis. The chapter emphasizes that creating trustworthy AI systems in healthcare requires more than just technical accuracy; it demands careful consideration of fairness, explainability, and privacy. The challenge of ensuring equitable healthcare delivery through AI is stressed, discussing methods to identify and mitigate bias in clinical predictive models. The chapter then delves into explainability as a cornerstone of human-centered CDSS. This focus reflects the understanding that healthcare professionals must not only trust AI recommendations but also comprehend their underlying reasoning. The discussion advances in an analysis of privacy vulnerabilities in medical AI systems, from data leakage in deep learning models to sophisticated attacks against model explanations. The text explores privacy-preservation strategies such as differential privacy and federated learning, while acknowledging the inherent trade-offs between privacy protection and model performance. This progression, from technical validation to ethical considerations, reflects the multifaceted challenges of developing AI systems that can be seamlessly and reliably integrated into daily clinical practice while maintaining the highest standards of patient care and data protection.

**Keywords** CDSS · AI · ML · explainability · fairness · privacy-preservation · probability calibration · decision curve analysis

---

\*Corresponding author, Fani Deligianni

# 1 Artificial Intelligence-Driven Clinical Decision Support Systems

## 1.1 From machine learning and statistical models to clinical decision support systems: An Overview

Clinical research demands a meticulous, multifaceted approach when evaluating predictive models, which extends beyond the traditional data science perspective. As we dive into this complex landscape, we must consider a series of key questions that shape the development and validation of machine learning models, ultimately determining their suitability as decision support systems in healthcare.

In prediction modeling, our main focus is on estimating the risk of adverse events based on a combination of factors. We seek to understand not only the predictive power of these factors, but also their individual contributions to the model's decision-making process. This understanding is crucial, as it allows us to incorporate subject matter knowledge into the modeling pipeline, bridging the gap between data-driven insights and clinical expertise.

The foundations of the clinical prediction model validation process have been presented in Steyerberg [Steyerberg and Vergouwe, 2014]. At the heart of this process lies the fundamental research question or hypothesis. For example, the choice of prediction outcome is paramount in clinical research. Outcomes such as mortality rates at 30 days are frequently relevant to various research questions. However, it's not just the nature of the outcome that matters, but also its frequency within the dataset. This frequency effectively determines the sample size, which in turn influences the statistical power and reliability of the model.

The selection of patient data for the development of the model is a critical consideration. Often, these data are collected for purposes other than the study at hand, raising questions about their representativeness. We must carefully examine whether patient records truly reflect the population for which the study is intended. Additionally, the treatment of prognostic factors and their effects presents a unique challenge. Although traditional studies often consider treatment effects negligible compared to prognostic factors, there are instances where these effects warrant specific attention. Adjusting for baseline prognostic factors can offer significant advantages in estimating treatment effects applicable to individual patients.

The reliability and completeness of the predictor measurements pose another hurdle in model development. Incomplete datasets are common, with missing values for potential predictors. The approach to handling these missing data can significantly impact the model's performance and validity. Although complete case analysis – excluding patients with missing values – is a straightforward solution, it often results in the loss of significant information. More sophisticated methods, such as imputation techniques that leverage correlations between variables, offer a more nuanced approach to preserving data integrity. In addition, informative missingness, where the fact that data are missing is related to the outcome of interest, must be carefully considered to avoid biased results.

As we navigate these considerations, we recognize that the development of machine learning models for clinical decision support systems is a multifaceted process. It requires a delicate balance between statistical rigor, clinical relevance, and practical applicability. By addressing these key questions and challenges, we pave the way for more robust and reliable predictive models that can enhance clinical decision-making and, ultimately, patient care.

## 1.2 A Quick Overview of Model Development and Validation Strategies of Machine Learning Models

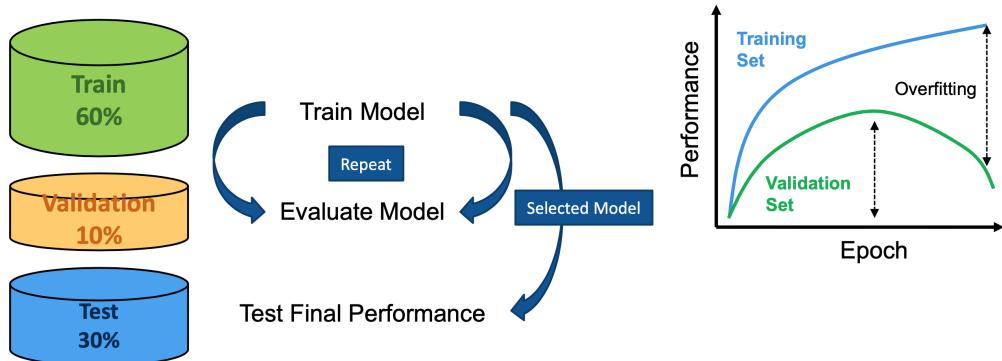


Figure 1: Model Development

Model evaluation and selection are critical steps in the machine learning development process. In an ideal scenario, we would have access to data that perfectly represents the entire target population. In this case, we could train and test the

machine learning model using the same data, and the error rate obtained would closely reflect the true error rate when the number of samples is very large. However, in reality, the error rate obtained when training and testing on the same dataset is positively biased. This is because the model has been exposed to the same data during both the training and testing phases, which can lead to an overly optimistic estimate of its performance. To address this issue, in real-world applications, it is important to split the available data into two separate sets: a training set and a testing set. Typically, around 70% of the data is used for training the model, while the remaining 30% is reserved for testing its performance on unseen examples. By separating the training and testing data, we can evaluate the model's ability to make accurate predictions on new, unseen data, which is crucial for deploying the model in real-world applications.

In most cases, we estimate the empirical risk based on a limited number of samples. This involves measuring the loss function with respect to our trained classifier, as discussed in [Japkowicz and Shah, 2011]. Empirical risk estimation is achieved by computing the average loss over the data points ( $m$  is the number of samples) according to a loss function  $L$ , which penalizes the differences between the predicted values  $f(x)$  and the actual targets  $y$ :

$$R_S(f) = \frac{1}{m} \sum_{i=1}^m L(y_i, f(x_i)) \quad (1)$$

Variations in the empirical risk estimation can arise from several factors. These include random variations in the training and testing sets, the learning algorithm itself, and even the noise inherent in the data classes being considered. One key advantage of the hold-out method (where the training and testing sets are independent) is that it provides some guarantees about the model's performance on data it has not been trained on before. However, we must also consider the confidence intervals around the empirical risk estimation. For example, when evaluating a machine learning algorithm, we should not assume a Gaussian distribution of the loss error, as the errors may be clustered near zero.

The error can be modeled using the Bernoulli distribution to calculate the error bound, Equation 2, providing an indication of the potential deviation between the empirical risk estimation and the true risk with a probability of accuracy of  $(1 - \delta)$ . In Equation 2,  $m'$  represents the sample size and  $\delta$  represents the confidence parameter, which quantifies the probability that our estimate is accurate.

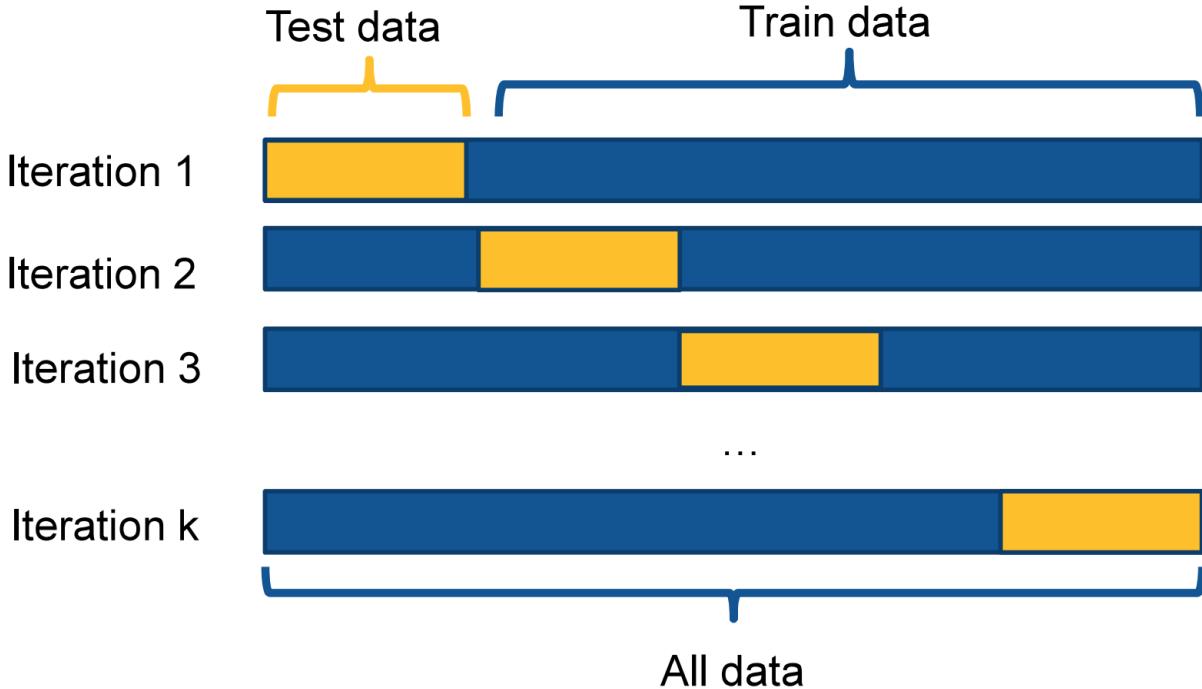
$$E = \sqrt{\frac{1}{2m'} \ln\left(\frac{2}{\delta}\right)} \quad (2)$$

The  $k$ -fold cross-validation is one of the most popular error estimation approaches in machine learning model training and evaluation. In this method, the dataset is divided into  $k$  distinct parts or "folds" like in Figure 2. During each iteration, one of these folds is reserved for testing, while the remaining  $(k - 1)$  folds are used for training the model. This process is repeated  $k$  times, with a different fold serving as the test set each time. By doing so, we obtain  $k$  separate estimates of the classifier's error rate. These estimates can then be averaged to give the mean performance of the algorithm across the different folds. Examining the variability of the error estimates across the  $k$  iterations can also provide valuable insights into the algorithm's stability and robustness. A key advantage of  $k$ -fold cross-validation is that the test samples are independent between the different folds, as there is no overlap. This helps to ensure a more reliable and unbiased assessment of the model's generalization capabilities.

A potential issue that can arise with standard  $k$ -fold cross-validation is that the data may not be evenly distributed across classes. This problem becomes worse when dealing with imbalanced class data, which is common in healthcare applications. To address this, we can employ a technique called stratified  $k$ -fold cross-validation. In this approach, the folds are created in a way that ensures the class distribution within each fold closely matches the original class distribution in the overall dataset.

A special case of  $k$ -fold cross-validation is leave-one-out cross validation (LOOCV). In this case, the value  $k$  is set to the number of samples in the dataset, meaning that each sample is used as the test set once while the remaining  $(k - 1)$  samples are used for training. LOOCV has the advantage of utilising most of the available data, which can result in relatively unbiased estimate of the model's performance. However, this comes at the cost of significant computational expense, especially as the dataset size grows. Although, LOOCV may provide better performance estimates in datasets with extreme values, it is important to note that this is not a guarantee of an unbiased classifier, especially when dealing with small datasets. The underlying assumption of LOOCV is that the training set is representative of the true data distribution, which may not always hold.

One key aspect of validation techniques such as  $k$ -fold cross-validation and LOOCV is that the estimate is not based on a single, fixed classifier. Instead, the model is retrained each time, producing a new classifier with each iteration. This approach has both advantages and disadvantages. The primary advantage is that it allows us to assess the stability of machine learning models across different data partitions. However, the disadvantage is that when comparing the

Figure 2:  $k$ -fold cross validation

performance of different algorithms, we must remember that we are comparing the average performance estimates of various classifiers, rather than a single, fixed classifier as in the holdout method. To address this, nested cross-validation is often used, as it provides a more robust estimate of model performance by incorporating an additional layer of cross-validation to tune hyperparameters, thereby reducing the risk of overfitting.

One way to describe the performance of classification algorithms is through a confusion matrix as in Figure 3b(a). This square matrix has rows and columns equal to the number of classes. The diagonal elements represent the true positives and true negatives, assuming "positive" refers to one class and "negative" to another. The off-diagonal elements indicate false positives and false negatives. From the confusion matrix, we can derive several performance metrics. For instance, accuracy is the ratio of correctly predicted observations to the total observations. Specificity, or the true negative rate, shows how well the classifier identifies negative cases, while recall also called sensitivity, or the true positive rate, indicates how well it identifies positive cases. Precision reflects the positive predictive value for a class. The F1 score combines recall and precision into a single metric, weighting them evenly.

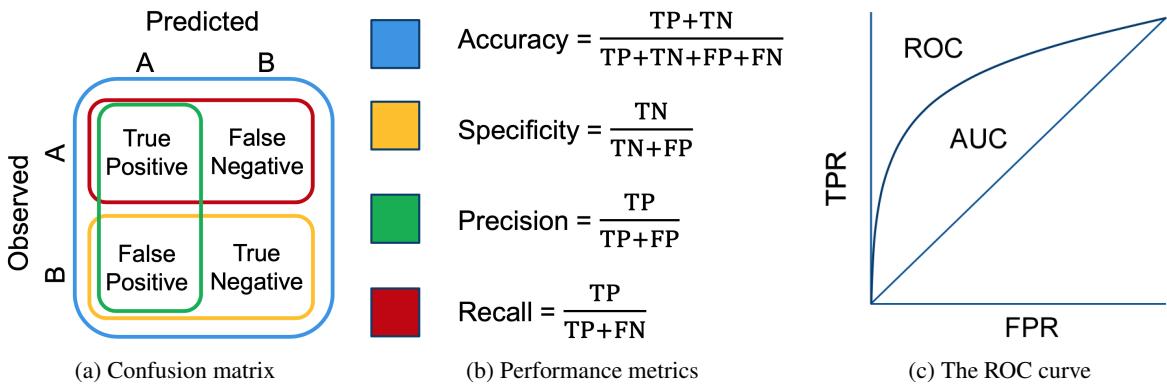


Figure 3: Performance evaluation of ML models.

An alternative method to assess the performance of a machine learning algorithm is by using a Receiver Operating Characteristic (ROC) curve, as shown in Figure 3c. The ROC curve plots the false positive rate on the horizontal axis and the true positive rate on the vertical axis. The true positive rate, or sensitivity, indicates how well the classifier identifies positive cases, while the false positive rate can be expressed as  $(1 - \text{specificity})$ . Thus, the ROC curve illustrates the trade-off between sensitivity and specificity for the classifier. It is generated by varying the threshold for classifying positive and negative cases. This makes the ROC curve a comprehensive measure of performance, as it considers different threshold settings. It is used not only to analyze the behavior of machine learning algorithms but also for model selection by identifying the optimal threshold region. For a random classifier, the ROC curve would be a straight diagonal line. The area under the curve (AUC) summarizes the classifier's performance, with higher values indicating better performance. The AUC is often used to compare different classifiers. Additionally, there are various extensions of the ROC and AUC for multi-class scenarios.

When comparing the performance of one algorithm against another, or multiple algorithms across one or more datasets, it is common to use null hypothesis statistical testing. Several statistical tests can validate the performance of two algorithms, but it is crucial to consider the assumptions underlying these tests. For instance, the paired t-test assumes a normal distribution, independence of measurements, and an adequate sample size. If the normality assumption is violated, non-parametric tests are often used. One such test is the Wilcoxon signed-rank test, an alternative to the paired t-test. This test is based on the ranks of the absolute differences, making it more robust to outliers. It is important to note that both parametric and non-parametric tests can be manipulated by increasing the number of samples, potentially affecting the results of the null hypothesis statistical testing approach.

### 1.3 Performance Validation in Clinical Decision Support Systems

Validation of prediction models tailored for clinical decision support systems should occur through both internal and external methods [Steyerberg and Vergouwe, 2014, Ramspeck et al., 2021]. Internal validation, using techniques like split-sample validation, cross-validation, or bootstrapping, assesses reproducibility within the development population. External validation, involving patients from different populations, tests the model's generalizability across various settings and demographics.

While internal validation techniques provide valuable insights into a model's performance, external validation serves as a crucial complement in assessing predictive models for clinical use. This process involves testing the model on data that is entirely separate from the development dataset, often collected from different institutions or time periods. Despite the growing number of publications on prediction models, studies employing both internal and external validation remain relatively scarce. This highlights the challenges in establishing predictive models as reliable decision support systems.

Figure 4 illustrates a risk prediction tool designed to estimate the likelihood of symptom nonremission in first-episode psychosis [Leighton et al., 2021]. The tool's internal validation performance was assessed using ten-fold cross-validation yielding an AUC of 0.74. External validation was conducted with patient data from various sites, produced an AUC of 0.73, confirming the model's generalisability. Successful external validation strengthens confidence in a model's clinical utility. It demonstrates that the model's predictions remain accurate across different patient populations and healthcare settings. This robustness is essential for establishing the model as a trustworthy component of clinical decision support systems. In other words, external validation offers a more rigorous test of a model's generalizability, revealing how well it performs in diverse real-world scenarios. It helps identify potential overfitting issues that may not be apparent through internal validation alone. In essence, external validation acts as a bridge between theoretical model development and practical clinical application. It provides the evidence needed to justify the integration of predictive models into healthcare decision-making processes, ultimately contributing to improved patient care and outcomes.

### 1.4 Calibration of Clinical Prediction Models

In clinical practice, the validation of machine learning models extends beyond traditional prediction performance metrics. While measures like AUC, precision, and F1 scores are crucial, they do not fully capture a model's clinical utility. Effective clinical decision support systems require assessment of underlying risk estimates and clinical usefulness, which can be subjective and application-dependent. Model calibration is a critical aspect of validation, referring to the agreement between observed outcomes and predictions [Van Calster et al., 2019]. For instance, if a model predicts a 15% risk of 30-day mortality, approximately 15 out of 100 patients with such a prediction should experience the outcome.

Calibration is typically assessed using flexible calibration curves, which plot estimated risks against observed proportions of events. Two key measures of calibration are the calibration-in-the-large (alpha) and calibration slope (beta). A well-calibrated model should have an alpha close to zero and a beta close to one. However, these measures alone do not

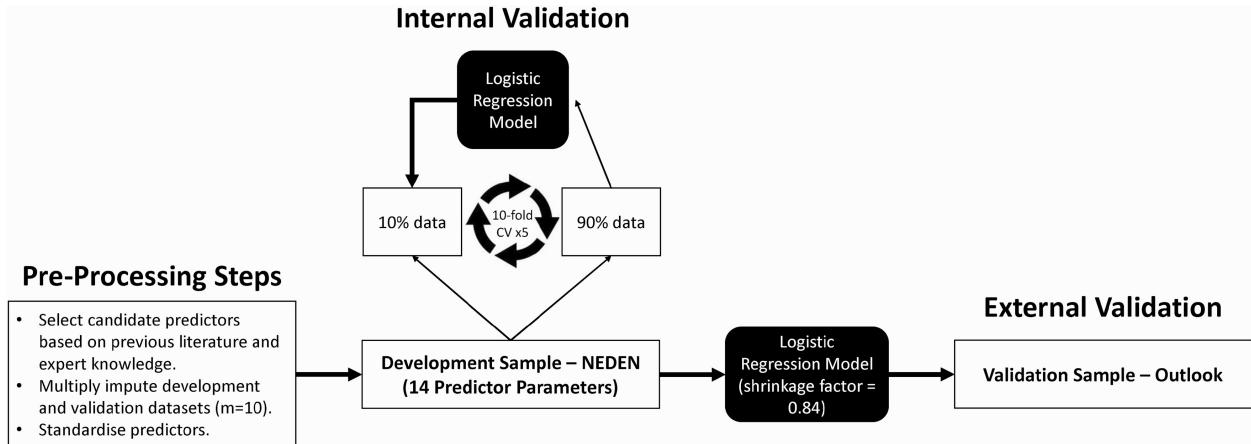


Figure 4: A Nonremission Risk Prediction Model in First-Episode Psychosis (reproduced with permission [Leighton et al., 2021])

guarantee perfect calibration across all risk levels. Visualization through calibration plots helps identify areas of over- or underestimation. Figure 5 shows the calibration curve for the regression model presented in Figure 4. This curve provides both qualitative and quantitative assessments of how well the developed risk prediction model aligns with the ideal calibration, represented by a blue line with a slope equal to 1.

Poor calibration can arise from various factors, including differences in patient characteristics or disease prevalence between development and validation populations, changes in healthcare practices over time, model overfitting, and measurement errors in medical data. Strategies to improve calibration include model refitting, continuous updating, and addressing population shifts dynamically. Sample size significantly impacts calibration assessment, with at least 200 events and non-events recommended for precise evaluation. In smaller datasets, evaluating moderate calibration through intercept and slope calculations may suffice.

The importance of calibration in clinical settings cannot be overstated. A poorly calibrated model, even with high discrimination, can lead to misleading or potentially harmful clinical decisions. For example, in the risk prediction of nonremission in first-episode psychosis, overestimation could falsely suggest that patients do not need medication, thereby exposing them to unnecessary risks.

## 1.5 Calibration in Deep Learning Models for Clinical Decision Support

Calibration is also a critical aspect of deep learning models in clinical decision support systems, particularly for establishing trustworthiness with users. A well-calibrated model provides confidence estimates that accurately reflect the probability of correct predictions. For instance, a model with 90% confidence should be correct 90 out of 100 times. In practice, perfect calibration is unattainable, but we aim to approximate it. The Expected Calibration Error (ECE) is a common metric used to assess calibration, measuring the difference between confidence and accuracy across prediction bins.

Recent studies have shown that deeper and more complex neural networks tend to be poorly calibrated, despite high accuracy [Guo et al., 2017, Nixon et al., 2019]. Interestingly, increasing model depth or the number of convolutional filters per layer tends to worsen calibration error while improving predictive performance. For example, a 110-layer ResNet model demonstrated high accuracy but poor calibration, potentially limiting its reliability as a decision support tool. The causes of miscalibration in deep networks are not fully understood, but they appear to correlate with model complexity and capacity. Conversely, techniques like weight decay (L2 regularization) can help reduce calibration error. These findings suggest that in complex networks, over-fitting may manifest in probability estimates rather than classification errors.

For healthcare applications, reliable confidence measures are crucial. Users of clinical decision support systems need to be aware of the confidence level in disease diagnostics. Efforts to improve calibration in deep neural networks include architectural modifications and adjustments to training and optimization strategies. While the ECE is widely used, it has limitations. The choice of bin number involves a bias-variance trade-off, and the metric may not fully capture calibration in multi-class problems. Additionally, it can be affected by cancellation effects between over- and under-confident predictions. Adaptive binning schemes have also been proposed to enhance the stability of calibration measurements.

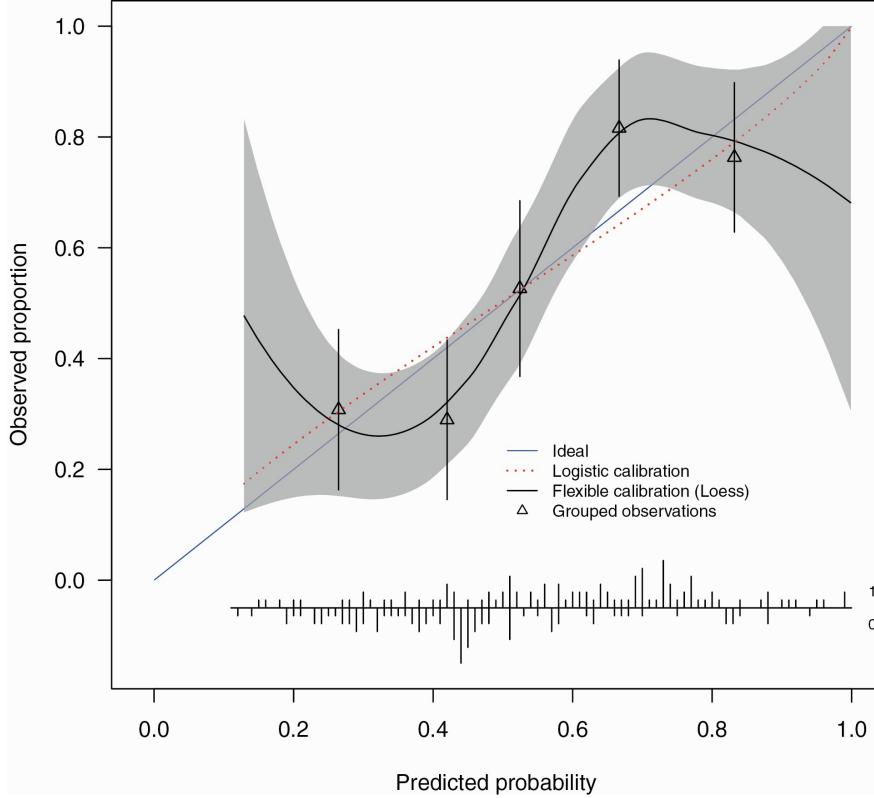


Figure 5: Probability calibration plot (reproduced with permission [Leighton et al., 2021])

In conclusion, while deep learning models can achieve high accuracy, their calibration remains a significant challenge. Addressing this issue is essential for developing trustworthy and effective clinical decision support systems. Future research should focus on refining calibration metrics and developing techniques to improve the reliability of confidence estimates in complex neural networks.

### 1.6 Decision Curve Analysis

While accuracy metrics such as sensitivity, specificity, and area under the receiver operating characteristic curve are essential for evaluating prediction models, they fail to capture the clinical consequences of implementing these models in practice. Decision curve analysis (DCA) addresses this limitation by incorporating the concept of net benefit (NB), allowing for a more comprehensive assessment of a model's clinical utility [Vickers and Elkin, 2006, Van Calster et al., 2018].

Net benefit is calculated across a range of threshold probabilities (ThresP), representing the point at which a clinician or patient would opt for intervention based on the model's prediction. This approach weighs the benefits of true positive (TP) predictions against the harms of false positives (FP), taking into account the relative importance of these outcomes in a given clinical context.

$$NB = \frac{TP}{N} - \frac{FP}{N} \times \frac{\text{ThresP}}{1 - \text{ThresP}} \quad (3)$$

DCA plots the net benefit against threshold probabilities, comparing the prediction model's performance to alternative strategies such as treating all patients or treating none [Vickers et al., 2019]. This visual representation allows stakeholders to assess the model's value across different risk thresholds, which may vary depending on the clinical scenario and individual preferences.

For instance, in cancer screening, a lower threshold probability might be preferred due to the severe consequences of missed diagnoses. Conversely, a higher threshold might be appropriate in situations where unnecessary interventions carry significant risks or costs. Figure 6 shows the DCA plot for the risk prediction model of nonremission presented

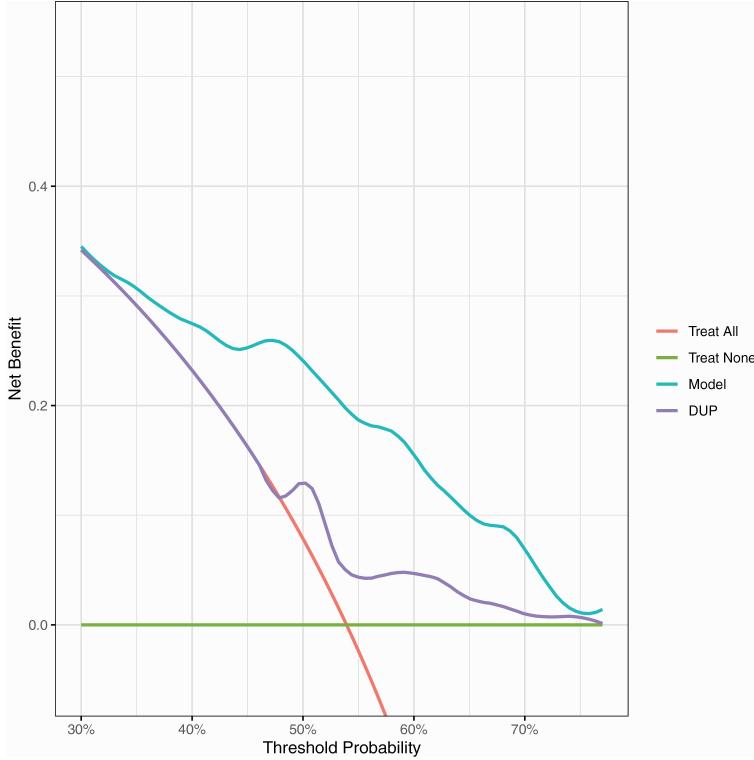


Figure 6: Understanding clinical consequences of a risk prediction of non-remission in first-episode psychosis based on Decision Curve Analysis (reproduced with permission [Leighton et al., 2021]).

in Figure 4. The plot demonstrates that the net benefit of using the developed model is higher than the alternatives of treating all, treating no patients, or treating based on the duration of untreated psychosis (DUP).

The interpretation of DCA results requires careful consideration of the clinical context. A model demonstrating higher net benefit than alternative strategies within a clinically relevant range of threshold probabilities can be considered clinically useful. However, this assessment should be made in conjunction with expert opinion and patient preferences.

DCA can be applied to both continuous probability predictions and binary diagnostic tests. It is particularly valuable when evaluating models in external validation cohorts, as it provides insights into the model's generalizability and potential impact on clinical decision-making.

An illustrative example of DCA in practice is its application to a prediction model for outcomes in first-episode psychosis [Leighton et al., 2019, 2021]. By consulting specialist psychiatrists to determine clinically relevant threshold probabilities, researchers were able to demonstrate the model's superior net benefit compared to alternative strategies within the specified range.

It's important to note that while DCA offers valuable insights into clinical utility, it should not replace traditional measures of model performance. Instead, it should be viewed as a complementary tool in the comprehensive evaluation of prediction models, bridging the gap between statistical performance and clinical applicability.

In conclusion, decision curve analysis provides a robust framework for assessing the clinical value of prediction models. By incorporating the concept of net benefit and allowing for comparison across different decision thresholds, DCA enables more informed decisions about model implementation in clinical practice. As healthcare continues to move towards personalized medicine, tools like DCA will play an increasingly crucial role in translating prediction models into meaningful clinical support systems.

## 1.7 Responsible Development of Artificial Intelligence-Driven Clinical Decision Support Systems

Previously, Steyerberg et al. [Steyerberg and Vergouwe, 2014] has established the importance of four steps to guide the development of machine learning models for healthcare applications: A) - Calibration in the large, B) Calibration slope, C) Discrimination performance established both with internal and external validation and D) Decision-curve analysis.



Figure 7: Ethical considerations for the use of AI in Clinical Decision Support Systems

Recently, the integration of artificial intelligence (AI) and in particular deep learning in clinical decision support systems necessitates a more careful consideration of the principles behind responsible model development [de Hond et al., 2022, Van Smeden et al., 2022]. These principles have extended guidelines to include additional safeguards that encompass fairness, explainability, privacy-preservation and interoperability, all of which are crucial for developing trustworthy AI applications in healthcare.

Figure 7 summarises the concepts behind responsible AI models in healthcare. We already referred to the term 'clinical usefulness', which encapsulates the necessity of an AI model to address a healthcare challenge and its capacity to evaluate if the advantages of an intervention justify the associated risks. 'Effective and Efficient' refers to the robustness of the underlying model and whether the outcome is reliably measured as it was highlighted at Steyerberg et al. [Steyerberg and Vergouwe, 2014]. 'Interpretability' is important to understand what the underlying factors are that the model based its specific decision. Interpretability and transparency are cornerstones of responsible AI, enabling users to understand both the technical processes and human decisions involved in the system's operation. Accountability in AI systems requires mechanisms to minimize negative impacts and report adverse consequences. In this context, transparency is crucial for assessing accountability and fairness.

Healthcare practitioners have expressed concerns about over-reliance on AI systems they cannot fully understand or explain. Addressing these concerns requires further training for practitioners and involving end-users in the design process. The next generation of human-centered clinical decision support systems should possess two key abilities: explaining the model's representation and decisions, and adapting based on feedback.

On the other hand, privacy and data governance are also paramount in clinical decision support systems. Developers must implement safeguards to protect user privacy, ensure data integrity, and control access to sensitive information. 'Privacy-preserving' technologies are also essential to address concerns arising from the use of AI models in new applications that enable real-time tracking of human activity and health in home settings. Privacy-preserved AI model should leverage interoperable solutions that seamlessly integrate into the healthcare system.

In conclusion, adherence to responsible AI development guidelines is crucial in designing AI-powered clinical decision support systems. Emphasizing clinical usefulness, explainability, and human-in-the-loop designs is essential to mitigate risks and realize the full potential of AI in healthcare. The development of the right level of interactivity and explainability in medical applications remains an open research question, highlighting the ongoing challenges in this rapidly evolving field.

## 2 ‘Fairness’ in Machine Learning Models

### 2.1 Assessing Bias in Clinical Predictive Models

Electronic health records (EHRs) present unique challenges and opportunities in predictive modeling, particularly in ensuring fairness and equity in healthcare outcomes. Biases can stem from flaws in study design, execution, or data

analysis. To identify such biases, a comprehensive approach is necessary, considering the model's intended use, target population, predictors, and predicted outcomes.

Therefore, the evaluation of predictive models should extend beyond discrimination and calibration to encompass potential biases that may introduce systematic errors. A framework for assessing bias in clinical predictive models has been proposed, focusing on four key domains: participant selection, variable and predictor selection, outcome assessment, and analysis [Wolff et al., 2019]. This framework emphasizes the importance of appropriate inclusion and exclusion criteria, consistent predictor definition and assessment across participants, and the use of standardized outcome definitions.

Additionally, the analysis should consider sample size adequacy, handling of continuous and categorical predictors. Researchers are advised to avoid selecting predictors based solely on univariate analysis. Models can be categorized as having low, medium, or high risk of bias based on the assessment of these domains. Notably, prediction models developed without external validation should generally be considered high risk, except when based on very large datasets.

The concept of "informative presence" in EHRs refers to the potential information carried by the presence or absence of patient data at any given time point. For example, EHRs can be inherently biased because sicker individuals are monitored more frequently. This type of informative presence, indicates that the frequency of health records can reflect a patient's health status. "Informative observation" extends this concept to the timing, frequency, and patterns of longitudinal observations in EHRs, which can provide insights into a patient's evolving health state [Sisk et al., 2021]. While these phenomena can complicate causal or association studies, they also offer potential sources of implicit information that could be exploited in predictive models.

In conclusion, while identifying and addressing bias is crucial for developing robust clinical predictive models, the inherent characteristics of EHRs, such as informative presence and observation, present both challenges and opportunities. Researchers must carefully interpret results while also exploring innovative ways to leverage these implicit data patterns to improve prediction accuracy.

## 2.2 Equity Challenges in Machine Learning for Healthcare Applications

The pursuit of health equity is a global priority, as exemplified by the World Health Organization's vision of a society where all individuals enjoy long, healthy lives [Amri et al., 2021]. Machine learning algorithms have the power to identify unexpected patterns in data, but they can also inadvertently perpetuate and amplify existing biases. This is particularly concerning when these algorithms are used to support clinical decision-making, as they can systematically disadvantage certain population groups [Barocas and Selbst, 2016, Obermeyer et al., 2019].

Electronic health records, which serve as the foundation for many predictive models, often reflect historical biases in patient selection, policies, and societal circumstances. These biases can manifest in various ways, such as under-representation of minority groups in the data, systematic differences in feature availability across populations, or the compounding of initial biases over time.

The case of St. George Hospital in the UK serves as a cautionary tale [Schwartz, 2019]. In the 1980s, the hospital developed a computer program to streamline medical school admissions based on historical data. Unintentionally, this program formalized existing prejudices against racial minorities and women, demonstrating how algorithmic decision-making can perpetuate systemic biases.

Similar issues have been observed in other domains, such as facial recognition technology and online advertising. These examples highlight the potential for algorithms to discriminate based on race, gender, or age, often due to non-representative training data or the inadvertent use of biased proxies.

In healthcare, a 2019 study revealed that a widely-used risk prediction algorithm considered Black patients to be healthier than equally ill White patients [Obermeyer et al., 2019]. This discrepancy arose because the algorithm used healthcare costs as a proxy for health needs, failing to account for disparities in healthcare access and utilization. Consequently, Black patients had to be significantly sicker than White patients to receive the same level of care.

This case underscores the importance of critically examining clinical decision support tools for potential biases. Even when sensitive attributes like race or gender are explicitly excluded from models, they can be implicitly correlated with other features, leading to discriminatory outcomes.

Discriminatory bias in healthcare algorithms can stem from various sources, including study design, data collection, clinician interactions, and patient behaviors. These biases may manifest as label bias, cohort bias, or various forms of data bias, such as minority under-representation or missing data for protected groups.

The interaction between clinicians and predictive models can also introduce biases. Automation bias may lead to over-reliance on model predictions, while dismissal bias could result in ignoring alerts for certain groups. Patient interactions with healthcare systems can further complicate matters, with issues like privilege bias and informed mistrust affecting model effectiveness and fairness.

Addressing algorithmic bias in healthcare is challenging. Simply removing sensitive fields from the data is insufficient, as algorithms can identify and learn from proxy variables. Moreover, the complex nature of these biases makes them difficult to detect and eliminate, particularly when they reflect deeply ingrained societal prejudices.

In conclusion, while machine learning holds great promise for advancing healthcare, it is crucial to remain vigilant about the potential for algorithmic bias. Researchers and practitioners must actively work to quantify and mitigate these biases, ensuring that predictive models promote rather than hinder health equity. This requires ongoing investigation, diverse and representative datasets, and a commitment to fairness in algorithm design and implementation.

### 2.3 Strategies to Ensure Fairness in Machine Learning Models for Healthcare

The pursuit of fairness in machine learning for healthcare applications is crucial, as algorithmic bias can lead to discriminatory outcomes that impact patient care. This section explores systematic approaches to detect and mitigate such biases.

Recent legislation, such as the 2019 Algorithmic Accountability Act in the United States [MacCarthy, 2020], has begun to address these concerns by requiring companies to assess and rectify algorithmic biases. However, the complexity and proprietary nature of many algorithms pose challenges for independent evaluation.

To mitigate discriminatory bias, several strategies have been proposed:

- Careful selection and representation of protected groups in the data.
- Thorough investigation of potential healthcare disparities in historical data.
- Incorporation of fairness goals into model training.
- Continuous evaluation of fairness metrics and model performance across groups.
- Vigilant monitoring of data and model reassessment during deployment.

Furthermore, several fairness metrics have been proposed [Beutel et al., 2019, Majumder et al., 2023]. Calibration techniques, applied within protected subgroups, can help identify algorithmic bias. Quantifying calibration bias within protected subgroups and assessing statistical parity are essential steps in evaluating model fairness. However, it is crucial to recognize that statistical parity may not be clinically meaningful when disease prevalence differs between subgroups. Other important metrics include independence, separation, and sufficiency [Carey and Wu, 2023]. Independence aims for classifier scores to be independent of group membership, while separation focuses on the independence of scores and sensitive variables conditional on the target variable. Sufficiency examines the independence of the target and sensitive variables given a particular score.

It is important to note that these fairness criteria cannot all be satisfied simultaneously when risk prevalence differs across groups. This highlights the need for careful consideration of trade-offs in AI model development. Therefore, further key objectives for fair decision-making in healthcare are defined that include achieving equal patient outcomes, equal model performance, and equal resource allocation across protected groups. However, these goals may sometimes conflict, necessitating thoughtful prioritization and stakeholder involvement in the design process.

In conclusion, ensuring fairness in machine learning models for healthcare is an ongoing challenge that requires continued research, vigilance, and collaboration among stakeholders. By addressing these issues systematically, we can work towards more equitable and effective healthcare systems that benefit all patients, regardless of their demographic characteristics.

## 3 Explainability as a central component of Human-Centred CDSS

### 3.1 Interpretability vs Explainability

Interpretability and explainability, while often used interchangeably, have distinct meanings in machine learning. Interpretability is an inherent model property, whereas explainability involves methods to elucidate non-interpretable models. Figure 8 illustrates a network assessing patient risk based on factors like BMI, age, smoking habits, alcohol consumption, and blood pressure. Consider an 85-year-old female patient with a BMI of 32, high blood pressure, and no smoking or alcohol use. The system labels her 'at risk' recommending medication. However, this output alone may not

suffice for a doctor to trust and act upon the model's decision. Understanding the reasoning behind the model's output becomes crucial, highlighting the importance of explainability in complex models, especially in critical domains like healthcare where comprehending the decision-making process is essential for informed and ethical treatment decisions.

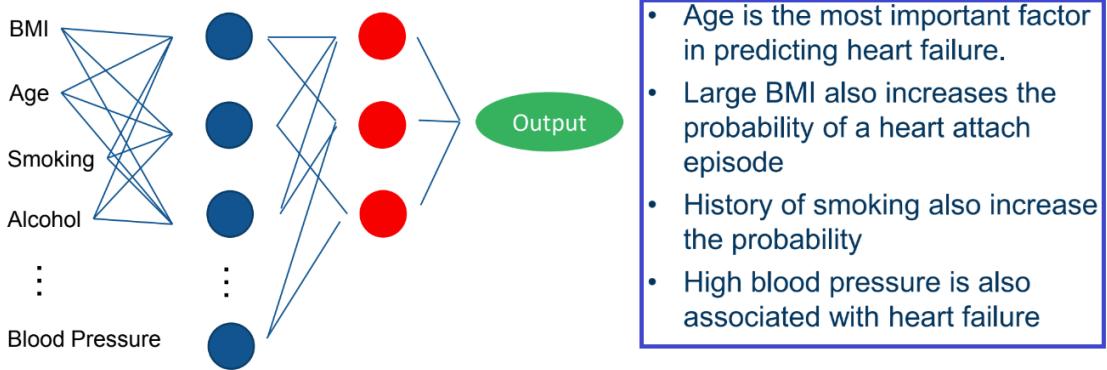


Figure 8: An example network with some specific input factors

Explainability in machine learning models can address crucial questions about a model's performance, success conditions, and decision factors. For example, consider that in heart failure prediction age is a significant factor, with individuals over 60 years having an estimated likelihood of 60%. Furthermore, a BMI exceeding 25 increases risk by 20%, as does smoking for over a decade. High blood pressure is also correlated with heart failure. An explainable model should identify these key input factors and quantify their impact on the decision. This insight into the model's underlying function aids result interpretation, clarifies decision-making processes, and helps understand model failures in noisy conditions. Essentially, explainability provides transparency into the model's inner workings, enabling users to comprehend not just what the model predicts, but why it makes those predictions.

Decision trees are widely regarded as highly interpretable machine learning models due to their transparent and intuitive structure as the example at Figure 9 shows. The tree-like representation clearly illustrates the decision-making process, with each node representing a specific decision point based on a particular feature. This allows users to easily follow the path from root to leaf, understanding how the model arrives at its predictions. The clear criteria used at each node for splitting the data provide insight into precisely how decisions are made at each step. This hierarchical nature lends itself well to visual representation, making it easier for both experts and non-specialists to grasp the model's logic. For any given prediction, one can trace the exact path through the tree, observing which features were considered and how they influenced the final output. This traceability enhances accountability and facilitates debugging. Moreover, the structure of the tree inherently reveals which features are most important for classification or regression, as they appear closer to the root and in more splits. Unlike more complex models, decision trees can be explained to individuals without a background in machine learning or statistics, facilitating communication between data scientists and stakeholders. However, it is important to note that interpretability can decrease as tree depth increases. Very deep trees may become more challenging to interpret, potentially approaching the complexity of "black box" models.

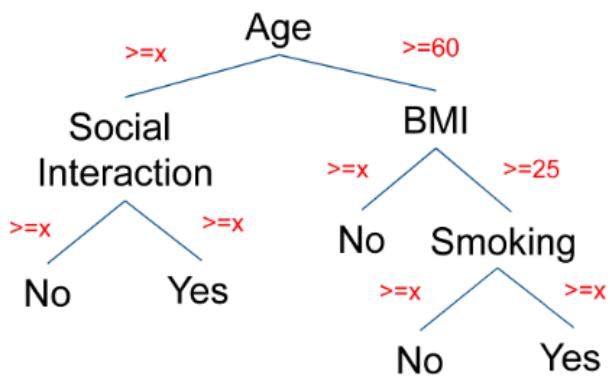


Figure 9: An example of a decision tree

Figure 10 provides a simplified overview of interpretable and explainable models. On the left, we see inherently interpretable models such as decision trees, linear regression, and logistic regression. These models have been widely used in clinical practice and decision-making due to their simple construction and easily understandable results. The straightforward nature of these models allows practitioners to readily interpret their outputs and understand the reasoning behind decisions. Consequently, these models do not require additional methods to explain their results, as their decision-making process is transparent by design. This intrinsic interpretability distinguishes them from more complex models that may require additional explanation techniques to elucidate their outputs.

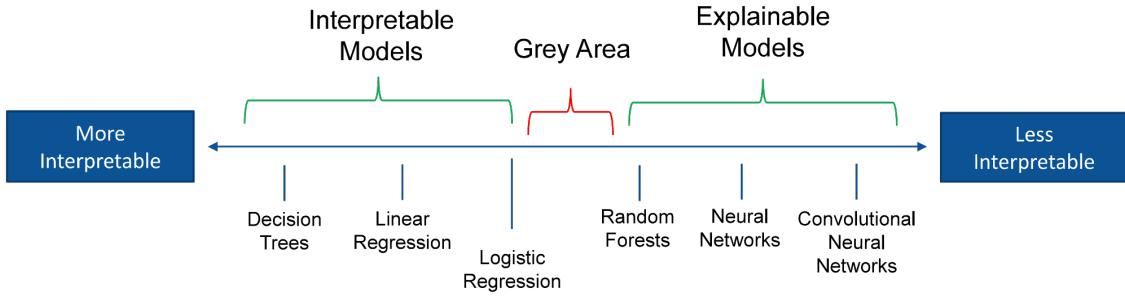


Figure 10: Interpretable vs explainable models

While linear regression and decision trees offer high interpretability, they often fall short in performance, especially given the complexity of modern datasets and available computational resources. Sacrificing predictive accuracy for inherent interpretability is increasingly seen as suboptimal in many applications. Instead, the focus has shifted towards developing methods to explain high-performing, complex models. This approach aims to harness the superior predictive power of sophisticated algorithms while still providing insights into their decision-making processes.

### 3.2 'Explainability' in Healthcare Applications

In healthcare applications, explainability is particularly critical for assessing model stability, visualizing relationships affecting outcomes, and enabling ethical analysis, especially concerning minority groups. It also facilitates patient involvement in decision-making processes and allows for the evaluation of privacy risks associated with complex model representations. This transparency is essential for maintaining the confidence of healthcare professionals, patients, and end-users. Moreover, explainability aids in monitoring model performance over time, as data distributions may shift and affect outcomes.

The significance of explainability extends to various stakeholders. Clinicians require trustworthy models that contribute to scientific knowledge. Patients need assurance of fair treatment and absence of hidden biases. Data scientists and developers utilize explainable models for debugging and improving product efficiency. Management must ensure regulatory compliance, while regulatory bodies need to certify model adherence to legislation.

Explainability is associated with several key objectives, including trustworthiness, causality inference, transferability, informativeness, confidence, fairness, accessibility, interactivity, and privacy awareness. While an explainable model may not guarantee absolute trust or prove causality, it can provide valuable insights into potential causal relationships and help validate results from other inference techniques.

### 3.3 Taxonomy of Explainability Methods

Some of the most common categorisations of explainability methods are local versus global, model agnostic versus model specific, data modality specific versus data modality agnostic and ad-hoc versus post-hoc explanations [Arrieta et al., 2020, Molnar, 2020, Stiglic et al., 2020]. Local versus global explanation is a very common distinction that translates on whether we get an explanation that relates to the overall function of the model, or an explanation related to specific decisions. Model agnostic versus model specific categorization is also very common [Ribeiro et al., 2016]. An important difference is that model agnostic explanations are not bound to a specific machine learning algorithm, whereas model specific explanations are derived directly based on the machine learning model employed.

Explainability methods can also be categorized based on the modality in the form of data modality specific versus data modality agnostic methods. In this case, the complexity of data representation is highlighted. For example, explaining decisions with relation to imaging data require a completely different approach than explaining differences in tabular data as they do not have any spatio-temporal dependency between variables. Another categorisation is for ad-hoc versus post-hoc explanations. While ad-hoc explanations aim in achieving interpretability by restricting the complexity of

the machine learning model (intrinsic explainability), post-hoc methods aim in achieving interpretability by applying methods that analyse the model after training.

Figure 11a presents a two-dimensional taxonomy of explainability methods, organized along two axes: local versus global explanations, and model-specific versus model-agnostic approaches. For example, Shapley Additive Explanation (SHAP) provides both local and global interpretability by analyzing variable impacts through perturbation - locally for individual predictions and globally for overall model behavior. In contrast, class activation maps and integrated gradients provide model-specific interpretability by analyzing neural network activations. These methods trace how specific input features influence the network's decision-making process for individual samples, revealing the internal reasoning patterns of the model.

Permutation feature importance is one of the simplest, yet powerful approaches that links the input variable with the outcome across all the samples and for this reason it is considered a global explainability method. Permutation based approaches such as permutation feature importance permutes the input values and features in order to understand the importance of each input variable [Mi et al., 2021]. In other cases, they can apply a surrogate model, an inherently interpretable model that is simple enough to understand its behaviour in a local space. The local importance highlights the important features for any individual prediction. It is very helpful to illustrate the local behaviour of the underlying model. Sometimes we can aggregate an average result from local methods in order to get a better idea of how the model functions globally [Jones et al., 2020, Mayourian et al., 2024].

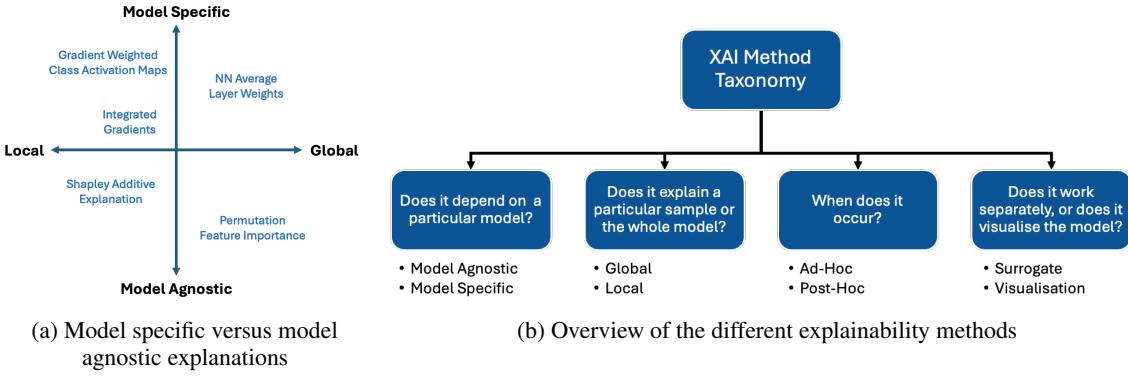


Figure 11: Explainability methods.

The advantage that a model-agnostic explanation provides is that we can compare different models with the same data and get an idea of the quality of the prediction as well as the explanation. Model agnostic tools are usually applied after the model has been trained, so they are considered as post-hoc explanations. In ad-hoc explanations, the model has been designed to be intrinsically explainable. Such an example is representation learning where the model identifies latent factors that intuitively have an explanation and they relate to the function of the model.

On the other hand, we can also categorize methods based on whether they are surrogate models or attribution based methods. Surrogate models basically try to use a simpler model to approximate the behaviour of a black box. Attribution methods can be also categorized based on whether they are perturbation based or back propagation or gradient based methods.

Figure 11b illustrates the key dimensions for categorizing explainability methods in AI systems. These dimensions include model dependency (agnostic vs. specific), scope of explanation (global vs. local), timing (intrinsic vs. post-hoc), and approach (surrogate models vs. visualization). Each dimension guides the selection of appropriate explainability techniques based on specific analysis requirements. The diverse taxonomy of explainability approaches yields varied types of model interpretations. Complex AI systems, particularly those serving diverse users, often require multiple complementary explainability methods to provide comprehensive insights into model behavior.

### 3.4 Evaluating Explainability in Clinical Decision Support Systems

The evaluation of explainability methods in clinical decision support systems is a crucial aspect of their development and deployment. This process considers not only the technical aspects of the explanations but also their effectiveness for end-users, whether they are healthcare providers, clinicians, patients or carers.

Explanations typically provide three types of information: the importance of features or attributes to the model, including their interactions; the reasoning behind specific predictions; and an approximation of the complex model using a simpler, interpretable surrogate model such as rule-based systems, decision trees, or linear models.

The evaluation of explanations involves assessing both the model's intrinsic interpretability and the quality of its approximation by interpretable explanations. Key aspects of this assessment include clarity (consistency of rationale for similar instances), parsimony (complexity and compactness of the explanation), fidelity (accuracy in describing the task model), and soundness (truthfulness to the task model).

Attribution-based explanations, which identify the input features most relevant to the model's decision, are common in post hoc explanation methods. While these explanations may not fully satisfy the sufficiency property, they often meet the parsimony criterion if the features are understandable to humans. For clinicians, such explanations are valuable in comparing the model's decision-making process with their own clinical knowledge.

User-based evaluation, both quantitative and qualitative, is crucial in understanding how trust in AI models affects overall system performance in human-in-the-loop scenarios. This approach bridges the gap between technical performance and practical utility in clinical settings, ensuring that explainable AI systems not only perform well mathematically but also integrate effectively into clinical workflows and decision-making processes. Toward this end, quantitative evaluations often utilize metrics based on questionnaires assessing the usefulness, satisfaction, and interest provided by the system's explanations. They may also measure human-machine task performance in terms of accuracy and response time.

## 4 Privacy Concerns in Clinical Decision Support Systems: A brief overview

### 4.1 Leakage and privacy concerns of deep learning models

The integration of machine learning in healthcare applications, particularly in clinical decision support systems (CDSS), necessitates understanding and addressing significant privacy concerns. Advanced machine learning models can memorise and inadvertently expose sensitive information, even when identity data has been removed or pseudo-anonymized. Furthermore, with state-of-the-art sensing technologies, it is now possible to monitor people 24/7 at home for healthcare applications [Yang et al., 2023]. This capability introduces new privacy challenges, as information about people's activities and physiology can be leaked in real-time [Zakariyya et al., 2024]. For example, wifi and radar-based human motion sensing has gained significant attention for offering unobtrusive observation in sensitive environments like assisted living facilities, hospitals, and residential settings. However, emerging research has uncovered a critical privacy concern: advanced radar systems can now accurately identify individuals through their unique walking patterns. These findings challenge the initial assumption of radar sensing as a privacy-preserving technology, highlighting the urgent need for robust privacy protection mechanisms in sensing systems, even when the raw data may not be visually comprehensible to humans. This section explores the inherent risks in deep learning models and discusses strategies to mitigate privacy threats in the context of healthcare applications.

Deep learning models excel at processing complex, correlated sensing data, which has led to substantial improvements in fields such as computer vision and information retrieval. However, these models inadvertently memorize training data within their weights, making it possible to reconstruct parts of the original dataset from the algorithm itself [Hartley et al., 2023]. Traditional anonymization techniques, such as removing personally identifiable information or using pseudo-anonymization, are insufficient protection against sophisticated privacy attacks against deep neural networks. These powerful algorithms can determine an individual's identity by exploiting similarities to other datasets or inferring information from remaining data points. This capability has led to large-scale re-identification attacks.

Privacy threats in machine learning can manifest in various sophisticated ways, even with limited model access. For example, memorisation of the training data might be reflected in assigning high likelihood to specific input samples. An attacker might gain insights into a model through its architecture, weights, training data, or even just its output logits. In the context of membership inference attacks (MIA), adversaries can potentially determine whether a specific data record was part of the original training dataset. The attack typically involves an attacker model that learns to predict the outcomes of the target model, with the goal of reconstructing sensitive input data.

While seemingly straightforward, MIA attacks serve as a foundational technique for more advanced data extraction methods via model inversion and reconstruction. The attack process often employs a shadow model, which is a surrogate model with similar architecture as the target model but different parameters [Shokri et al., 2017]. By generating synthetic data and evaluating its performance against the shadow model, the attacker can identify data likely similar to the original training set. This method is particularly powerful when the attacker lacks direct access to the target model's training data. A high prediction score from the shadow model suggests that the synthetic data closely resembles the original target data [Carlini et al., 2022].

To address these concerns, innovative approaches are being developed. One promising method involves disentangling latent representations in data, separating key features from identity information [Malek-Podjaski and Deligianni, 2021, Li et al., 2024]. This approach has shown success in improving classification performance while protecting individual privacy, as demonstrated in recent work on human pose data. Other potential mitigation mechanisms include incorporating robust privacy techniques during the development of the target model to enhance its resistance to data leakage attacks.

In summary, the powerful memorization capabilities of deep neural networks create inherent vulnerabilities that can compromise patient privacy. It is essential to safeguard user privacy by integrating robust privacy protection mechanisms early in the development of decision support systems. Tools like privacy-meter available at [Murakonda and Shokri, 2020] can facilitate this process by measuring how an AI system may potentially leak sensitive information. By separating biometric data from features of interest and filtering out identity information early in the processing pipeline, it is possible to enhance both the effectiveness and the privacy-preserving qualities of these systems.

## 4.2 Defenses against privacy attacks

Privacy preservation in healthcare machine learning applications is crucial, both at the data and model levels. This section explores various approaches to protect patient privacy, contrasting centralized and federated learning methods.

### 4.2.1 Differential Privacy Against privacy attacks

**Differential Privacy (DP)** is a mathematical framework designed to protect sensitive data used in training AI models. DP algorithms mitigate the risk of data leakage by introducing calibrated noise into computations. This is particularly valuable when handling sensitive information, such as healthcare data, in the development of decision support systems. The procedure involves adding noise based on two privacy budget parameters,  $\epsilon$  and  $\delta$  [Dwork et al., 2014]. The parameter  $\epsilon$  controls the amount of noise added, while  $\delta$  defines the probability of the mechanism failing to maintain privacy. Stronger privacy guarantees are achieved with smaller values of  $\epsilon$  and  $\delta$ .

**Definition 1:** A randomized function  $F$  provides pure  $\epsilon$ -DP if for all neighbouring input datasets  $D_1$  and  $D_2$  differing on at most one element and  $\forall S \subseteq \text{Range}(F)$  [Dwork et al., 2014], satisfying equation 4 below, where  $\Pr$  in equations 4 and 5 represents a probability measure.

$$\Pr[F(D_1) \in S] \leq e^\epsilon \Pr[F(D_2) \in S] \quad (4)$$

For  $(\epsilon, \delta)$ -DP, the guarantee is relaxed as follows:

$$\Pr[F(D_1) \in S] \leq e^\epsilon \Pr[F(D_2) \in S] + \delta \quad (5)$$

Thus, when  $\delta = 0$ , the relaxed guarantee simplifies to the pure  $\epsilon$ -DP condition. The noise introduced can follow either a Gaussian or Laplace distribution, depending on the desired balance between privacy guarantees and utility. DP techniques are extensively utilized to develop robust machine learning models that protect training data from leakage, especially in the presence of MIA. In this context, noise can be introduced to either the data or the model gradients during training.

DP methods that focus on input data features often rely on the addition of Laplace noise [Phan et al., 2017, Fujimoto et al., 2023, Zakariyya et al., 2024]. Proper implementation of additive noise injection on specific features effectively safeguards sensitive data against MIA [Zakariyya et al., 2024].

Another widely adopted mechanism for creating DP-compliant models is applying  $(\epsilon, \delta)$ -DP to model gradients during training [Abadi et al., 2016, Dupuy et al., 2022, Boenisch et al., 2024]. This approach involves clipping gradients and adding Gaussian noise proportional to  $\epsilon$  at each training iteration. The clipping norm, a fixed threshold ( $C$ ), bounds the gradient magnitudes for individual data points, managing the effect of large gradients [Kong and Munoz Medina, 2024]. The model is iteratively trained using mini-batches of the input data samples and a stochastic gradient descent (SGD) algorithm, commonly referred to as the DP-SGD procedure. Algorithm 1 outlines the DP-SGD training procedure, incorporating gradient clipping and noise addition to ensure DP guarantee.

**Algorithm 1** Differentially Private Stochastic Gradient Descent (DP-SGD)

**Input:** Dataset  $\mathcal{D} = \{x_1, \dots, x_n\}$ , loss function  $\mathcal{L}$ , learning rate  $\eta$ , clipping norm  $C$ , noise scale  $\sigma$ , batch size  $B$ , number of iterations  $T$ .

**Output:** Model parameters  $\theta_T$ .

- 1: Initialize model parameters  $\theta_0$ .
- 2: **for**  $t = 1$  to  $T$  **do**
- 3:   Sample a random mini-batch  $\mathcal{B}_t \subset \mathcal{D}$  of size  $B$ .
- 4:   **for each**  $x_i \in \mathcal{B}_t$  **do**
- 5:     Compute the gradient  $\mathbf{g}_i = \nabla_{\theta} \mathcal{L}(\theta_{t-1}, x_i)$ .
- 6:     Clip the gradient:  $\tilde{\mathbf{g}}_i = \mathbf{g}_i / \max\left(1, \frac{\|\mathbf{g}_i\|_2}{C}\right)$ .
- 7:   **end for**
- 8:   Aggregate the clipped gradients:  $\bar{\mathbf{g}} = \frac{1}{B} \sum_{i \in \mathcal{B}_t} \tilde{\mathbf{g}}_i$ .
- 9:   Add noise:  $\hat{\mathbf{g}} = \bar{\mathbf{g}} + \mathcal{N}(0, \sigma^2 C^2 \mathbf{I})$ .
- 10:   Update the model:  $\theta_t = \theta_{t-1} - \eta \hat{\mathbf{g}}$ .
- 11: **end for**
- 12: **return**  $\theta_T$

#### 4.2.2 Federated Learning and Defenses Against Privacy Attacks

Traditionally, machine learning models in healthcare have been developed in centralized settings, where both data and models reside within the same environment [Alanazi, 2022]. For instance, the MIMIC database, a clinical database integrating information from thousands of patients exemplifies such centralized approaches. Similarly, technology corporations like Google collect usage data directly from mobile devices for training models. While these methods are effective in leveraging large datasets, they also raise significant privacy concerns.

Federated learning has emerged as an alternative decentralized approach for building machine learning models. This paradigm involves a single server and multiple clients, each retaining their own data. Instead of centralizing data, the algorithm is distributed to where the data resides. Training iterations occur locally on the clients, with model parameters shared with a centralized server that aggregates these updates to create a global model [McMahan et al., 2017]. A commonly used federated learning algorithm is Federated Averaging (FedAvg) [McMahan et al., 2017]. FedAvg enables the creation of a global model by using a central server to average the weights of local models from various client devices. This process is iterative: during each communication round, the server interacts with clients to update the global model until convergence is achieved.

Federated learning allows data to remain with its owners while still enabling collaborative algorithm training. However, it can be communication and memory intensive. Additionally, federated learning alone does not inherently guarantee security and privacy, necessitating additional protective measures. Both centralized and edge models are vulnerable to privacy and adversarial attacks [Kaassis et al., 2024, Song et al., 2020, Kumar et al., 2023].

Model-level defenses include machine unlearning (or "forgetting"), which aims to remove specific data without retraining the entire model. This approach, while conceptually appealing, faces challenges in implementation and verification. Adversarial defenses, such as adding targeted noise to confidence score vectors, have been proposed to protect against MIA, though they lack theoretical privacy guarantees [Jia et al., 2019].

DP has gained significant attention in federated learning due to its ability to provide a guaranteed maximum privacy loss. In federated learning, this method involves adding calibrated noise to model updates during local training on each device, enhancing both generalization and patient privacy. However, determining appropriate privacy thresholds for local model updates remains a challenge.

Homomorphic encryption represents another promising avenue for secure AI in healthcare, allowing data processing without decryption [Kaassis et al., 2024]. However, its computational complexity is prohibitive for practical applications and it also suffers from a lack of explainability and transparency. Despite these challenges, it offers strong privacy guarantees and it is considered a key element in next-generation secure and private AI systems.

Ultimately, the goal is to strike an optimal balance between accuracy, explainability, fairness, and privacy in healthcare AI systems. While federated learning and other privacy-preserving methods offer promising solutions, they must be carefully combined and implemented to ensure both the utility and security of sensitive healthcare data. Several open questions remain in this field. Researchers are exploring whether decentralized data storage and federated learning can enable cross-institutional research while preserving privacy.

### 4.3 Adversarial attacks against explanations in Deep Learning

Explainability techniques in deep neural networks, aimed at improving interpretability and trust, are increasingly recognized as being susceptible to adversarial attacks [Baniecki and Biecek, 2024]. This section examines the vulnerabilities of these techniques and their potential implications for healthcare applications, where trust and reliability are paramount.

Recent research has revealed that explanations for deep learning models can be manipulated in ways that are difficult to detect. Two main types of attacks have been identified: those that manipulate the model's loss function to produce misleading explanations while preserving performance, and those that introduce small, nearly imperceptible perturbations to input data to alter explanations significantly. Popular adversarial attacks targeting explainability models include both white-box and black-box approaches [Baniecki and Biecek, 2024, Vadillo et al., 2024]. White-box attacks operate under the assumption that the adversary has complete knowledge of the model's architecture, parameters, and gradients. Examples of white-box attacks include the Fast Gradient Sign Method (FGSM) [Goodfellow et al., 2014], its iterative variant, the Projected Gradient Descent (PGD) [Kurakin et al., 2016], and the Carlini & Wagner (C&W) attack [Carlini and Wagner, 2017]. These methods leverage detailed internal information to craft adversarial examples that maximize model vulnerability.

In contrast, black-box attacks are designed for scenarios where the attacker lacks access to the model's internal parameters or architecture. These attacks are often query-based, relying on input-output observations to infer model behavior. A notable example is the Zero Order Optimization (ZOO) attack [Chen et al., 2017], which uses iterative querying to approximate gradients and generate adversarial examples.

Both attack paradigms aim to manipulate model gradients, creating adversarial inputs that lead to misclassifications. Such attacks pose significant risks to the security and robustness of AI systems, particularly in sensitive applications where model integrity is important.

Gradient-based explanation methods, such as Grad-CAM, are particularly susceptible to manipulation. Researchers have demonstrated various techniques to fool these methods, including:

- Location fooling: Making the explanation highlight a specific region of the input, regardless of its relevance.
- Top-k fooling: Reducing the importance of pixels that originally had the highest interpretation scores.
- Center-mass fooling: Optimizing the heatmap to diverge as much as possible from the original without affecting classification performance.
- Active fooling: Swapping explanations between different target classes entirely.

These manipulations are achieved by introducing additional terms to the loss function during training, balancing between classification accuracy and explanation manipulation.

Research has identified potential defenses. One approach involves smoothing explanations at the network level by replacing rectified linear unit (ReLU) activation functions with softplus functions. The smoothness of these functions, controlled by a beta parameter, can be adjusted to make networks more resistant to data perturbation-based manipulations. DP can also help protect against privacy attacks on explanations.

Understanding and modeling the susceptibility of neural networks to explanation manipulation is crucial. It not only helps in preventing malicious attacks but also in detecting when explanations might be misleading due to other limitations. This knowledge can guide the development of more robust explainability techniques, which is particularly important in healthcare applications where the reliability of AI-assisted decisions is paramount.

### 4.4 Trade-offs Between Privacy Protection and Model Performance

The implementation of privacy-preserving techniques in machine learning introduces a fundamental tension between data protection and algorithmic performance. This delicate balance is particularly critical in healthcare applications, where both privacy and predictive accuracy are paramount. Privacy-preserving methods fundamentally challenge the traditional approach to machine learning by introducing mechanisms that deliberately obscure and modify data or alter the convergence of the model training process. At the core of this challenge lies the complex interplay between protecting individual privacy and maintaining the integrity of predictive models. When privacy techniques are applied, they invariably reduce the richness and depth of available information, creating a nuanced landscape of compromises.

Feature representation suffers particularly from privacy sanitization techniques. By removing or masking sensitive identifying information, models lose critical contextual information that might be essential for accurate predictions.

In personalized medicine, this can mean overlooking subtle but important correlations that could significantly impact diagnostic accuracy.

Empirical research has demonstrated concrete performance implications. Differential privacy can reduce model accuracy by 5 to 20 percent, depending on the privacy budget. They are also notoriously difficult to train from scratch and thus they depend on pretrained models. Federated learning models often show a 3 to 15 percent performance reduction compared to centralized training approaches. Synthetic data generation presents even more significant challenges, potentially leading to up to 30 percent loss in predictive power if not meticulously implemented.

Despite these technical challenges, the ethical imperative remains clear. The potential psychological and social harm from data breaches far outweighs marginal improvements in predictive accuracy. Privacy protection must remain a fundamental consideration, not an afterthought. Ultimately, the goal is not to choose between privacy and performance, but to develop intelligent systems that can maintain both.

## 5 Conclusions

The integration of artificial intelligence into clinical decision support systems represents both a transformative opportunity and a complex challenge in healthcare. While these systems offer unprecedented capabilities for improving patient care, their successful implementation demands a careful balance of multiple critical factors. The development pathway must address not only technical excellence in model performance, but also robust validation, proper calibration, and thorough decision curve analysis. As we look to the future, the success of AI in healthcare will depend on our ability to navigate challenges in explainability, causality, and bias while maintaining the trust of both healthcare providers and patients.

The complexity of healthcare AI systems raises three paramount concerns that must be carefully balanced. First, there is the critical challenge of ensuring fairness and addressing bias, particularly given the inherent "informative presence" in electronic health records and their potential to reflect historical societal disparities. Second is the need for transparency and explainability, requiring sophisticated approaches that go beyond simple interpretability to provide meaningful insights for healthcare professionals and patients alike. Third is the fundamental requirement to protect patient privacy, particularly given the potential vulnerabilities created by deep learning models' ability to memorize training data. While techniques such as differential privacy, federated learning, and homomorphic encryption offer promising solutions, they often require careful trade-offs between privacy protection and model performance.

Success in this evolving landscape requires a holistic approach that considers these interconnected challenges. The path forward demands ongoing collaboration between technical experts, healthcare providers, and policymakers to develop systems that are not only technically sophisticated but also ethically sound, clinically useful, and privacy-preserving. As AI continues to transform healthcare, our ability to balance these competing demands while maintaining focus on improved patient outcomes will determine the ultimate impact of these innovations on the future of medicine.

**Acknowledgements** Fani Deligianni is supported by funding from EPSRC (EP/W01212X/1) and Academy of Medical Sciences (NGR1/1678). She is also a member of the research team for NIHR (NIHR158303). This chapter builds upon content from the Coursera specialization 'Informed Clinical Decision Making using Deep Learning'.

## References

- Ewout W Steyerberg and Yvonne Vergouwe. Towards better clinical prediction models: seven steps for development and an abcd for validation. *European heart journal*, 35(29):1925–1931, 2014.
- Nathalie Japkowicz and Mohak Shah. *Evaluating learning algorithms: a classification perspective*. Cambridge University Press, 2011.
- Chava L Ramspekk, Kitty J Jager, Friedo W Dekker, Carmine Zoccali, and Merel van Diepen. External validation of prognostic models: what, why, how, when and where? *Clinical Kidney Journal*, 14(1):49–58, 2021.
- Samuel P Leighton, Rajeev Krishnadas, Rachel Upthegrove, Steven Marwaha, Ewout W Steyerberg, Georgios V Gkoutos, Matthew R Broome, Peter F Liddle, Linda Everard, Swaran P Singh, et al. Development and validation of a nonremission risk prediction model in first-episode psychosis: an analysis of 2 longitudinal studies. *Schizophrenia bulletin open*, 2(1):sgab041, 2021.
- Ben Van Calster, David J McLernon, Maarten Van Smeden, Laure Wynants, Ewout W Steyerberg, Topic Group ‘Evaluating diagnostic tests, and prediction models’ of the STRATOS initiative Bossuyt Patrick Collins Gary S. Macaskill Petra McLernon David J. Moons Karel GM Steyerberg Ewout W. Van Calster Ben van Smeden Maarten Vickers Andrew J. Calibration: the achilles heel of predictive analytics. *BMC medicine*, 17(1):230, 2019.
- Chuan Guo, Geoff Pleiss, Yu Sun, and Kilian Q Weinberger. On calibration of modern neural networks. In *International conference on machine learning*, pages 1321–1330. PMLR, 2017.
- Jeremy Nixon, Michael W Dusenberry, Linchuan Zhang, Ghassen Jerfel, and Dustin Tran. Measuring calibration in deep learning. In *CVPR workshops*, volume 2, 2019.
- Andrew J Vickers and Elena B Elkin. Decision curve analysis: a novel method for evaluating prediction models. *Medical Decision Making*, 26(6):565–574, 2006.
- Ben Van Calster, Laure Wynants, Jan FM Verbeek, Jan Y Verbakel, Evangelia Christodoulou, Andrew J Vickers, Monique J Roobol, and Ewout W Steyerberg. Reporting and interpreting decision curve analysis: a guide for investigators. *European urology*, 74(6):796–804, 2018.
- Andrew J Vickers, Ben van Calster, and Ewout W Steyerberg. A simple, step-by-step guide to interpreting decision curve analysis. *Diagnostic and prognostic research*, 3:1–8, 2019.
- Samuel P Leighton, Rachel Upthegrove, Rajeev Krishnadas, Michael E Benros, Matthew R Broome, Georgios V Gkoutos, Peter F Liddle, Swaran P Singh, Linda Everard, Peter B Jones, et al. Development and validation of multivariable prediction models of remission, recovery, and quality of life outcomes in people with first episode psychosis: a machine learning approach. *The Lancet Digital Health*, 1(6):e261–e270, 2019.
- Anne AH de Hond, Artuur M Leeuwenberg, Lotty Hooft, Ilse MJ Kant, Steven WJ Nijman, Hendrikus JA van Os, Jiska J Aardoom, Thomas PA Debray, Ewoud Schuit, Maarten van Smeden, et al. Guidelines and quality criteria for artificial intelligence-based prediction models in healthcare: a scoping review. *NPJ digital medicine*, 5(1):2, 2022.
- Maarten Van Smeden, Georg Heinze, Ben Van Calster, Folkert W Asselbergs, Panos E Vardas, Nico Bruining, Peter De Jaegere, Jason H Moore, Spiros Denaxas, Anne Laure Boulesteix, et al. Critical appraisal of artificial intelligence-based prediction models for cardiovascular disease. *European heart journal*, 43(31):2921–2930, 2022.
- Robert F Wolff, Karel GM Moons, Richard D Riley, Penny F Whiting, Marie Westwood, Gary S Collins, Johannes B Reitsma, Jos Kleijnen, Sue Mallett, and PROBAST Group†. Probast: a tool to assess the risk of bias and applicability of prediction model studies. *Annals of internal medicine*, 170(1):51–58, 2019.
- Rose Sisk, Lijing Lin, Matthew Sperrin, Jessica K Barrett, Brian Tom, Karla Diaz-Ordaz, Niels Peek, and Glen P Martin. Informative presence and observation in routine health data: a review of methodology for clinical risk prediction. *Journal of the American Medical Informatics Association*, 28(1):155–166, 2021.
- Michelle M Amri, Geneviève Jessiman-Perreault, Arjumand Siddiqi, Patricia O’Campo, Theresa Enright, and Erica Di Ruggiero. Scoping review of the world health organization’s underlying equity discourses: apparent ambiguities, inadequacy, and contradictions. *International Journal for Equity in Health*, 20(1):70, 2021.
- Solon Barocas and Andrew D Selbst. Big data’s disparate impact. *Calif. L. Rev.*, 104:671, 2016.
- Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, 366(6464):447–453, 2019.
- Oscar Schwartz. Untold history of ai: Algorithmic bias was born in the 1980s. *IEEE Spectrum*, 15, 2019.
- Mark MacCarthy. *An examination of the Algorithmic Accountability Act of 2019*. SSRN, 2020.

- Alex Beutel, Jilin Chen, Tulsee Doshi, Hai Qian, Allison Woodruff, Christine Luu, Pierre Kreitmann, Jonathan Bischof, and Ed H Chi. Putting fairness principles into practice: Challenges, metrics, and improvements. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, pages 453–459, 2019.
- Suvodeep Majumder, Joymallya Chakraborty, Gina R Bai, Kathryn T Stolee, and Tim Menzies. Fair enough: Searching for sufficient measures of fairness. *ACM Transactions on Software Engineering and Methodology*, 32(6):1–22, 2023.
- Alycia N Carey and Xintao Wu. The statistical fairness field guide: perspectives from social and formal sciences. *AI and Ethics*, 3(1):1–23, 2023.
- Alejandro Barredo Arrieta, Natalia Díaz-Rodríguez, Javier Del Ser, Adrien Bennetot, Siham Tabik, Alberto Barbado, Salvador García, Sergio Gil-López, Daniel Molina, Richard Benjamins, et al. Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai. *Information fusion*, 58:82–115, 2020.
- Christoph Molnar. *Interpretable machine learning*. Lulu. com, 2020.
- Gregor Stiglic, Primoz Kocbek, Nino Fijacko, Marinka Zitnik, Katrien Verbert, and Leona Cilar. Interpretability of machine learning-based prediction models in healthcare. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 10(5):e1379, 2020.
- Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. Model-agnostic interpretability of machine learning. *arXiv preprint arXiv:1606.05386*, 2016.
- Xinlei Mi, Baiming Zou, Fei Zou, and Jianhua Hu. Permutation-based identification of important biomarkers for complex diseases via machine learning models. *Nature communications*, 12(1):3008, 2021.
- Yola Jones, Fani Deligianni, and Jeff Dalton. Improving ecg classification interpretability using saliency maps. In *2020 IEEE 20th International Conference on Bioinformatics and Bioengineering (BIBE)*, pages 675–682. IEEE, 2020.
- Joshua Mayourian, William G. La Cava, Akhil Vaid, Girish N. Nadkarni, Sunil J. Ghelani, Rebekah Mannix, Tal Geva, Audrey Dionne, Mark E. Alexander, Son Q. Duong, and John K. Triedman. Pediatric ecg-based deep learning to predict left ventricular dysfunction and remodeling. *Circulation*, 149(12):917–931, 2024. doi:10.1161/CIRCULATIONAHA.123.067750. URL <https://www.ahajournals.org/doi/abs/10.1161/CIRCULATIONAHA.123.067750>.
- Shufan Yang, Julien Le Kernev, Olivier Romain, Francesco Fioranelli, Pierre Cadart, Jérémie Fix, Chenfang Ren, Giovanni Manfredi, Thierry Leterre, Israel David Hinostroza Sáenz, et al. The human activity radar challenge: benchmarking based on the ‘radar signatures of human activities’ dataset from glasgow university. *IEEE Journal of Biomedical and Health Informatics*, 27(4):1813–1824, 2023.
- Idris Zakariyya, Linda Tran, Kaushik Bhargav Sivangi, Paul Henderson, and Fani Deligianni. Differentially private integrated decision gradients (idg-dp) for radar-based human activity recognition. *arXiv preprint arXiv:2411.02099*, 2024.
- John Hartley, Pedro P Sanchez, Fasih Haider, and Sotirios A Tsaftaris. Neural networks memorise personal information from one sample. *Scientific Reports*, 13(1):21366, 2023.
- Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, pages 3–18. IEEE, 2017.
- Nicholas Carlini, Steve Chien, Milad Nasr, Shuang Song, Andreas Terzis, and Florian Tramer. Membership inference attacks from first principles. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1897–1914. IEEE, 2022.
- Matthew Malek-Podjaski and Fani Deligianni. Towards explainable, privacy-preserved human-motion affect recognition. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 01–09, 2021. doi:10.1109/SSCI50451.2021.9660129.
- Zhi Li, Daichi Amagata, Yihong Zhang, Takahiro Hara, Shuichiro Haruta, Kei Yonekawa, and Mori Kurokawa. Mutual information-based preference disentangling and transferring for non-overlapped multi-target cross-domain recommendations. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval*, pages 2124–2133, 2024.
- Sasi Kumar Murakonda and Reza Shokri. MI privacy meter: Aiding regulatory compliance by quantifying the privacy risks of machine learning. *arXiv preprint arXiv:2007.09339*, 2020.
- Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Foundations and Trends® in Theoretical Computer Science*, 9(3–4):211–407, 2014.
- NhatHai Phan, Xintao Wu, Han Hu, and Dejing Dou. Adaptive laplace mechanism: Differential privacy preservation in deep learning. In *2017 IEEE international conference on data mining (ICDM)*, pages 385–394. IEEE, 2017.

- Ryusei Fujimoto, Yugo Nakamura, and Yutaka Arakawa. Differential privacy with weighted  $\epsilon$  for privacy-preservation in human activity recognition. In *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 634–639. IEEE, 2023.
- Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. Deep learning with differential privacy. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 308–318, 2016.
- Christophe Dupuy, Radhika Arava, Rahul Gupta, and Anna Rumshisky. An efficient dp-sgd mechanism for large scale nlu models. In *ICASSP 2022-2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 4118–4122. IEEE, 2022.
- Franziska Boenisch, Christopher Mühl, Adam Dziedzic, Roy Rinberg, and Nicolas Papernot. Have it your way: Individualized privacy assignment for dp-sgd. *Advances in Neural Information Processing Systems*, 36, 2024.
- Weiwei Kong and Andres Munoz Medina. A unified fast gradient clipping framework for dp-sgd. *Advances in Neural Information Processing Systems*, 36, 2024.
- Abdullah Alanazi. Using machine learning for healthcare challenges and opportunities. *Informatics in Medicine Unlocked*, 30:100924, 2022.
- Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Aguera y Arcas. Communication-efficient learning of deep networks from decentralized data. In *Artificial intelligence and statistics*, pages 1273–1282. PMLR, 2017.
- Georgios A. Kaassis, Marcus R. Makowski, Daniel Rückert, and Rickmer F. Braren. Secure, privacy-preserving and federated machine learning in medical imaging. *Nature Machine Intelligence*, 2024.
- Mengkai Song, Zhibo Wang, Zhifei Zhang, Yang Song, Qian Wang, Ju Ren, and Hairong Qi. Analyzing user-level privacy attack against federated learning. *IEEE Journal on Selected Areas in Communications*, 38(10):2430–2444, 2020.
- Kummarji Naveen Kumar, Chalavadi Krishna Mohan, and Linga Reddy Cenkeramaddi. The impact of adversarial attacks on federated learning: A survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 46(5):2672–2691, 2023.
- Jinyuan Jia, Ahmed Salem, Michael Backes, Yang Zhang, and Neil Zhenqiang Gong. Memguard: Defending against black-box membership inference attacks via adversarial examples. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 259–274, 2019.
- Hubert Baniecki and Przemyslaw Biecek. Adversarial attacks and defenses in explainable artificial intelligence: A survey. *Information Fusion*, page 102303, 2024.
- Jon Vadillo, Roberto Santana, and Jose A Lozano. Adversarial attacks in explainable machine learning: A survey of threats against models and humans. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, page e1567, 2024.
- Ian J Goodfellow, Jonathon Shlens, and Christian Szegedy. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412.6572*, 2014.
- Alexey Kurakin, Ian Goodfellow, and Samy Bengio. Adversarial machine learning at scale. *arXiv preprint arXiv:1611.01236*, 2016.
- Nicholas Carlini and David Wagner. Towards evaluating the robustness of neural networks. In *2017 ieee symposium on security and privacy (sp)*, pages 39–57. Ieee, 2017.
- Pin-Yu Chen, Huan Zhang, Yash Sharma, Jinfeng Yi, and Cho-Jui Hsieh. Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models. In *Proceedings of the 10th ACM workshop on artificial intelligence and security*, pages 15–26, 2017.