



TWIN-GPT: Digital Twins for Clinical Trials via Large Language Model

Yue Wang^{1*} Tianfan Fu^{2*} Yinlong Xu¹ Zihan Ma¹ Hongxia Xu¹ Bang Du¹
Yingzhou Lu³ Honghao Gao⁴ Jian Wu¹ Jintai Chen^{5,+}

¹Second Affiliated Hospital School of Medicine, School of Public Health, Zhejiang University

²Computer Science Department, Rensselaer Polytechnic Institute

³School of Medicine, Stanford University

⁴School of Computer Engineering and Science, Shanghai University

⁵Computer Science Department, University of Illinois Urbana-Champaign

+ Corresponding author

Abstract

Clinical trials are indispensable for medical research and the development of new treatments. However, clinical trials often involve thousands of participants and can span several years to complete, with a high probability of failure during the process. Recently, there has been a burgeoning interest in virtual clinical trials, which simulate real-world scenarios and hold the potential to significantly enhance patient safety, expedite development, reduce costs, and contribute to the broader scientific knowledge in healthcare. Existing research often focuses on leveraging electronic health records (EHRs) to support clinical trial outcome prediction. Yet, trained with limited clinical trial outcome data, existing approaches frequently struggle to perform accurate predictions. Some research has attempted to generate EHRs to augment model development but has fallen short in personalizing the generation for individual patient profiles. Recently, the emergence of large language models has illuminated new possibilities, as their embedded comprehensive clinical knowledge has proven beneficial in addressing medical issues. In this paper, we propose a large language model-based digital twin creation approach, called **TWIN-GPT**. **TWIN-GPT** can establish cross-dataset associations of medical information given limited data, generating unique personalized digital twins for different patients, thereby preserving individual patient characteristics. Comprehensive experiments show that using digital twins created by **TWIN-GPT** can boost the clinical trial outcome prediction, exceeding various previous prediction approaches. Besides, we also demonstrate that **TWIN-GPT** can generate high-fidelity trial data that closely approximates specific patients, aiding in more accurate result predictions in data-scarce situations. Moreover, our study provides practical evidence for the application of digital twins in healthcare, highlighting its potential significance.

1 Introduction

Clinical trials serve as essential research investigations in the field of prospective medicine. They are designed to rigorously evaluate the safety and efficacy of new treatments (e.g., drugs, or medical devices). Despite playing a pivotal role in advancing medical knowledge and enhancing patient care, these trials typically engage tens to thousands of human participants and frequently extend over several years, hindering the progress of research and development. There is an increasing interest in leveraging artificial intelligence models to predict trial outcomes, leveraging electronic health records (EHR) and significantly accelerating the pace of research [58, 26, 36, 22]. Learning from EHR data, models are able to identify the relationship between potential health issues with personalized characteristics, thus excelling at forecasting disease occurrence and even developing personalized treatment plans [61, 49].

Existing approaches leveraging EHR for clinical trial outcome prediction still face a set of challenges. These methods often fail to account for individual differences between patients and variations among diseases, resulting in predictions that may not align with real-world scenarios [36, 22]. EHR-based clinical trial outcome prediction models typically suffer from two key problems: **(1) Data Gap:** the disconnect between the data and its related realistic background knowledge makes it hard to leverage the supportive knowledge in prediction. **(2) Data Inconsistency:** discrepancies between data from different sources, presenting different data distributions, different patterns of data missing, and different data recording formats, undermine the reliability of prediction results across datasets.

Digital twin creation technology has exhibited great potential in clinical practice [15, 29], simulating patient physiological state [43, 11], disease progression [78], and treatment effects [1, 13]. These technologies leverage historical and real-time data to provide medical professionals with more accurate and comprehensive personalized health information, introducing opportunities in outcome prediction and analysis. Inspired by this, Das *et al.* [30] designed a simple model for cancer patients' EHR digital twin creation, which promotes privacy protection and the outcome prediction in clinical trial simulation. However, this method only relies on the existing datasets when creating digital

twins, which fails to leverage knowledge beyond the dataset and limits the accuracy of clinical trial outcome prediction. Traditional digital twin models still face challenges in achieving accurate clinical trial outcome predictions, failing to effectively address data gaps and data inconsistencies. Data gaps are particularly prominent in trial predictions due to variations in ICD codes for different medications and diseases, necessitating the acquisition of real-world background knowledge by the digital twin for clinical trials. Moreover, the data inconsistency problem is greatly exacerbated in EHR data for clinical trial scenarios, posing a challenge to digital twin creation, since EHRs for clinical trials often originate from different sites and thus present greater inconsistencies.

To address these problems, in this paper, we propose a novel approach based on LLMs that creates digital twins to enhance the effectiveness and accuracy of clinical trial outcome prediction. Often referred to as ‘world models’, LLMs possess not only extensive language understanding capabilities but also a comprehensive understanding of world knowledge, including medical knowledge. This makes LLMs capable of overcoming the aforementioned data gap and inconsistency problems. Our proposed innovative model TWIN-GPT is fine-tuned on a pre-trained LLM (ChatGPT [55]) on clinical trial datasets, so as to generate personalized digital twins for different patients. According to the virtual personalized patient data (i.e., digital twins) generated by TWIN-GPT based on historical and real-time examination results, we find that patients’ physiological and pathological states over the clinical trial duration can be accurately forecasted, thereby achieving more precise trial outcome predictions. Moreover, experiments on real-world datasets demonstrate that our TWIN-GPT can account for individual patient variations and disease complexities, producing data that closely aligns with diverse real-world scenarios. It resolves challenges of data gap and inconsistency in EHR while ensuring the protection of patient privacy. Our main contributions are summarized as follows:

- **Innovative Integration of LLM for Digital Twin Creation:** To the best of our knowledge, we are the first to integrate LLM into digital twin creation and perform knowledge association across datasets, which effectively imputes missing EHR data and provides a more personalized patient modeling approaches, thus addressing the limitations of traditional models.
- **Enhanced Personalization and Accuracy:** TWIN-GPT harnesses the vast medical knowledge embedded within ChatGPT to generate personalized digital twin models for individual patients. Experimental findings showcase that this approach achieves significantly enhanced personalization by accounting for each patient’s unique characteristics and disease complexities, thereby improving the accuracy of predicted clinical trial outcomes.
- **Privacy Protection and Versatility in Application:** Our TWIN-GPT approach also protects the patient privacy by generating virtual patient data and simulating personalized physiological measures over time, minimizing the use of sensitive patient information. The versatility allows for application across various clinical trial scenarios, thereby accelerating the pace of clinical trials and enhancing medical research and patient care [30].

2 RELATED WORK

2.1 Large Language Models (LLMs) for Medicine

LLMs have exhibited excellent performance on various tasks, especially in the field of medicine [64, 28, 47]. The current research on LLMs in the medical field has provided novel applications in bedside diagnosis, automated drafting of clinical documents, and improving medical workflow efficiency [12, 56, 53]. LLMs have demonstrated their utility in clinical applications by passing medical licensing exams and offering superior empathy and quality of medical advice compared to human clinicians [71, 44, 54, 63, 73, 77, 75]. In clinical applications, LLMs were used to facilitate the analysis of large amounts of textual data, providing insights that can drive medical discoveries and increase the efficiency of research workflows [68, 69, 62, 4]. They also have significant advantages in daily clinical tasks like clinical documentation drafting, and can significantly reduce the administrative burden on medical staff [80, 39, 10, 33]. However, there is no research using LLMs in clinical trial scenarios, which is a crucial area demanding the extensive medical knowledge encoded within these large language models.

2.2 Patient Outcome Prediction

Previous research in patient outcome prediction primarily relied on traditional machine learning methods such as decision trees, support vector machines, and logistic regression [23, 42, 14, 20]. These approaches often utilized manually selected features from high-dimensional clinical data. However, manual feature selection frequently fails to incorporate informative features, thereby failing to fully capture individualized patient information and complex data relationships [25]. Recently, deep learning methods have gained prominence with the advancement of deep learning technology. Researchers have begun to explore the use of neural networks for patient prediction [24, 58, 26, 46, 17, 19], which handle well with large-scale data and automatically select informative features, leading to significant achievements. Fu *et al.* [36, 35] proposed a hierarchical interaction network (HINT) to predict the clinical trial outcome based on

drug molecules, disease codes, eligibility criteria, etc. Lu *et al.* [50] enhance HINT from the perspective of uncertainty quantification and interpretability.

Among these, analysis of EHR data plays a crucial role in patient outcome prediction. Many studies have investigated how to effectively utilize EHR data for patient prediction [23, 41, 57, 75], applying long-term historical EHR learning, medical text mining, time-series data analysis [45, 2, 81]. Utilizing EHR data can provide comprehensive patient information, but it also suffer from data gap problem and data inconsistency problem. Recently, digital twin creation has emerged as a noteworthy field in EHR learning, offering new opportunity to patient outcome prediction [65]. Digital twin models can simulate a patient’s personalized physiological states, disease progression, and treatment effects based on historical EHR and real-time data [30].

2.3 EHR Data Generation

Data generation methods can create synthetic data that is effective in addressing data scarcity issues. EHR data generation methods often synthesize patient records conditioned on a patient’s historical data and distribution information, using techniques such as generative adversarial networks (GANs) [5, 25, 18] or variational auto-encoders (VAEs) [1, 7, 21, 37, 34]. The advantage of these methods is their ability to protect patient privacy, but ensuring the generated data maintains consistency with real data [59] remains a challenge.

To protect patient privacy, many approaches employ data masking and anonymization techniques in learning EHR data [38, 79, 67, 70]. These methods involve de-identifying or anonymizing sensitive information to create anonymous or partially anonymous data. While these methods provide privacy protection, they may potentially lead to a decrease in data quality [31, 8]. Model-driven generation methods use known patient models or epidemiological knowledge to generate synthetic EHR data. These models can take into account a patient’s physiological states, disease progression, and treatment effects, resulting in more accurate data generation [82, 9, 27]. Typically, these methods require domain experts’ knowledge to guide the generation process. Some data augmentation techniques can also increase data diversity and quantity using existing EHR data. This includes extracting information from medical texts using natural language processing techniques or creating new data points by combining different types of medical events [16, 74, 32, 76]. Data augmentation can enhance the training effectiveness of models but is still subject to limitations imposed by the original data.

Digital twin is a specialized method for generating personalized EHR data, ensuring similarity and correspondence with the original data, as well as guaranteeing patient privacy protection [51]. Das *et al.* [30] used a VAE to model digital twins in clinical trials to achieve prediction of patient outcome in low-data scenarios. Liu *et al.* [48] proposed a cloud healthcare system framework based on digital twin healthcare (CloudDTH), which is used to monitor, diagnose, and predict personal health to achieve the goal of personal health management. Zhong *et al.* [84] used ICU EHR data to build the ICU digital twin model to study critical care services in the ICU. However, these approaches only perform digital twinning within their datasets and do not solve the data gap and data inconsistency problems.

3 METHODOLOGY

In this section, we introduce TWIN-GPT, a novel approach that creates personalized digital twins for effective virtual clinical trial simulation, leveraging the power of large language models (LLMs) to address the challenges of clinical trials in limited data scenarios. Our method originates from the understanding that clinical trials are essential for medical research and drug development, but they are often hindered by the extensive time and participant involvement required. TWIN-GPT aims to revolutionize this by generating high-fidelity, personalized digital twins of patients, thus facilitating virtual clinical trials that can significantly enhance patient safety, expedite development, and reduce costs.

Overview. In Section 3.1, we define the problem of digital twin creation for clinical trials. Section 3.2, We employ a novel prompt-tuning approach to generate and update patient digital twins based on their EHR data, enhancing the model’s predictive accuracy and understanding of patient outcomes. In Section 3.3, We propose TWIN-GPT to generate digital twins of patients in clinical trials, enhancing prediction accuracy and understanding of patient outcomes by leveraging historical and similar patient data.

3.1 Problem Formulation and Overview Pipeline

We assume that there are a total of N participant patients in a clinical trial, and each patient n ’s trial encounters are encapsulated as

$$X_{n;1:T_n} = \{x_{n,1}, x_{n,2}, \dots, x_{n,T_n}\}, \quad (1)$$

where each $x_{n,t}$ is a collection of event types occurring at the t -th visit, defined as

$$x_{n,t} = \{x_{n,t}^1, x_{n,t}^2, \dots, x_{n,t}^u\}. \quad (2)$$

Each element $x_{n,t}^i$ corresponds to a kind of clinical event like a treatment or an adverse reaction, and u is the total number of all types of events, while $x_{n,t}^i = \{c_1, c_2, \dots, c_n\}$ represents the occurrence of event, where c_l is 1 or 0. Formally, we synthesize the digital twin of a patient by an auto-regressive model M , and each step predicts the next visit event:

$$\hat{X}_{n,t} = M\left(X_{n^{(\cdot)};1:t-1}, \{X_{n';1:t-1}\}_{n'=1}^{N'}, \Theta\right), \quad (3)$$

where $t = 1, \dots, T_n$, and Θ denotes the model parameters. The term N' is the count of nearest neighbor patients for reference in the digital twin generation. In the training process, we supervise the model M 's learning by comparing the generated digital twins with the true patient's trial encounters during the trial. The learning objective is to maximize the cosine similarity between real and synthetic patient representations,

$$\arg \max_{\Theta} \frac{1}{T_n} \sum_{t=1}^{T_n} \text{sim}(F_{n,t}, \hat{F}_{n,t}), \quad (4)$$

where $F_{n,t}$ and $\hat{F}_{n,t}$ denote the average representations of $x_{n,t}^u$ and $\hat{x}_{n,t}^u$ (where $\hat{x}_{n,t}^u$ is in $\hat{X}_{n;1}$) over the time span from 1 to T . We use cosine similarity as the similarity metric (i.e., "sim" in Eq. 4).

In our analysis, we particularly focus on three essential clinical events (i.e., u):

- *treatment*, $x_{n,t}^{\text{treat}}$, is the assigned treatment at the t -th timestep for the patient n ;
- *medication*, $x_{n,t}^{\text{med}}$, is defined as the treatment (i.e., drugs) given to patients in response to their current health conditions;
- *adverse event*, $x_{n,t}^{\text{ae}}$, refers to all unexpected health incidents that occur during patient visits.

To predict adverse events in the next visit, denoted as $X_{n,t+1}^{\text{ae}}$, we feed all three event types into the model as the *causality* among these event types is crucial for accurate prediction. For example, the doctor might provide medication *Docetaxel* to a patient at the timestep $t + 1$ due to the adverse events observed in the last visit. Meanwhile, the adverse event *pain* might not be observed at timestep $t + 1$ due to the medication *Docetaxel* given at timestep t . Since our model is a kind of large language model, the input three event types serve as in-context learning ability [52] in our case.

3.2 Prompt Tuning for Digital Twin in LLMs

In this work, we develop a large language model (LLM) to serve as the auto-regressive model M to perform the digital twin creation. To LLMs, a *prompt* is the initial input or query given to the model for generating a better response [83]. A context-suited prompt is beneficial to our digital twin creation task. Compared with expensive model tuning, prompt tuning is cheaper. We proposed a novel prompt-tuning approach to seek suitable prompts to generate better digital twins. The steps of our proposed *prompt tuning* are as follows:

- Initially, the first version of digital twin is generated based on the patient's EHR data. At this stage, the patient's EHR data of previous visits and the five most similar EHR data are provided as reference.
- Next, the real patient records (e.g., presenting the adverse event) are regarded as the ground truth to provide supervision. We use initial prompts for predicting adverse events and medications. Based on the ground truth data, the LLM's parameters are updated. The TWIN-GPT is developed on the ChatGPT, and we utilize ChatGPT's fine-tuning API to update it.
- If the correct adverse event under the current treatment is predicted, the medication for the next time is deduced sequentially.

Steps 1-3 are repeated each time the patient's EHR data is updated. When the updated EHR data is provided, along with another five most similar EHR profiles, the adverse events are predicted and medication is recommended again, as illustrated in table 1 below. The goal of this approach is to track and update the patient's EHR digital twin in real time, obtaining prompts that most easily establish knowledge associations between input and output.

3.3 Digital Twin Generation

In clinical trials, the sequence of real patient visit records is defined as $X_{n;1:T_n}$. Our goal is to generate a digital twin $\hat{X}_{n;1:T_n}$ that can retain the features of the target patient. For this purpose, we propose a generator, namely TWIN-GPT, that simulates personalized patient trajectories based on the real record $X_{n;1:T_n}$. The TWIN-GPT predicts in an auto-regressive manner,

$$\hat{X}_{n;T_n-1:T_n} = \text{TWIN-GPT}(X'_{n;1:T_n-1}, \{X_{k;1:T_k-1}\}_k). \quad (5)$$

Visit	Input	Prompt
t	Target visit: $X_{n;1:t-1}$ Five nearest neighbor EHR	Based on the historical visit data of the target patient: xxxxxx, please use the patient’s history and the k most similar visits to generate a digital twin of the target patient and predict the digital twin’s adverse events.
$t + 1$	Target visit: $X_{n;1:t}$ EHR Five nearest neighbor EHR	Based on the historical visit data of the target patient: xxxxxx, please use the patient’s history and the k most similar visits to generate a digital twin of the target patient and predict the digital twin’s recommended medications.

Table 1: Illustration of Prompt Tuning for Digital Twin.

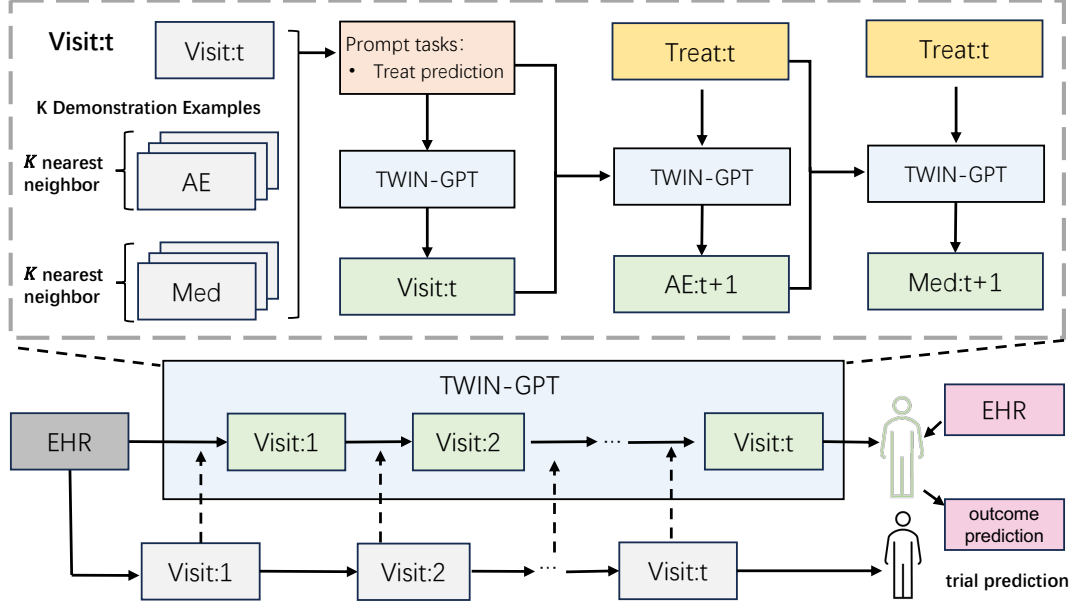


Figure 1: The workflow of TWIN-GPT. (Bottom) TWIN-GPT takes real follow-up visits $X_{n;1:T_n-1}$ of a patient and generates twin visits of next step, \hat{X}_{n,T_n} . Finally, the whole visit sequence can be predicted. (Top) The top part elaborates on how to use the digital twin visits $\hat{x}_{n,1:t}$ (at the time step t) to predict the events that occurred in the next timestamp $\hat{x}_{n,t+1}^{\text{event}}$. We use K nearest neighboring patient visits in TWIN-GPT fine-tuning but only use origin visits in prediction. “Treat”: treatment; “Med”: medication; “AE”: adverse event.

In training, $X'_{n;1:T_n-1}$ is $X_{n;1:T_n-1}$, while in test $X'_{n;1:T_n-1}$ is the previous prediction outcomes $\hat{X}_{n;1:T_n-1}$. To enable TWIN-GPT to learn personalized clinical trial data for patients and to leverage data association between different patients, we adopted the method of prompt tuning introduced above. In this way, we hope TWIN-GPT can accurately generate digital twin characteristics of the patient and finally realize the prediction of different clinical trials. We fine-tune TWIN-GPT following the step described in Sec. 3.2, letting it make predictions based on the patient’s historical visits so that TWIN-GPT can learn the patient’s unique characteristics. Specifically, based on the medication (*Med*) and treatment before and planned at the current time point t , the Adverse Event (*AE*) at the next time point $t + 1$ is predicted. Then based on the AE_{t+1} , the Med_{t+1} can be further predicted. Here, the patient’s unique characteristics and information from k similar patients are used as references, to ensure the reliability of the digital twins. Please note that in clinical trials, AEs and medication information are crucial factors we need to focus on, as they significantly impact the success and conclusions of the clinical study. Therefore, our TWIN-GPT is primarily designed to predict these two events.

Notably, different patients may have different trajectories in the trial. To enable TWIN-GPT to create digital twins for various patient patterns, the k most similar patients are retrieved based on all of their previous event sequential $X_{1:t}$. This approach not only helps improve TWIN-GPT’s comprehensive understanding of patient patterns but also prevents it from overfitting to specific individuals. Specifically, at the time step of the visit $x_{n,t}$, we enumerate all the other patients and retrieve K visits $\{x_{k,t_k}\}_{k=1}^K$ with the highest cosine similarity to $x_{n,t}$. Note that t_k can be either equal or unequal to t . By integrating these similar visits as inputs, TWIN-GPT can also enhance its ability to differentiate between similar visits in prediction. The overall workflow is illustrated in Fig. 1.

4 APPLICATION & EVALUATION

The generated digital twins are beneficial for simulating clinical trials in silico. In this section, we present two application scenarios (personalized generation and counterfactual generation) and evaluate the quality of the digital twins based on clinical trial outcome prediction accuracy and privacy protection.

4.1 Digital Twins Generation Application

4.1.1 Personalized Generation

Personalized Generation refers to the process of using EHR data to guide TWIN-GPT in replicating patients, ultimately generating digital twins. Throughout each step of this process, the model incorporates both its data and data from the k -nearest neighbors, enabling TWIN-GPT to perform the in-context learning.

4.1.2 Counterfactual Generation

The purpose of this task is to simulate the trajectories of patients under alternative treatment schedules, including switching a patient from the treatment arm (T) to the control arm (C). This simulation not only enhances patient records but also enables the estimation of personalized treatment effects. Moreover, it facilitates the balancing of trial data for predictive modeling while substantially reducing the necessary sample size for recruiting participants in the control arm. To generate the counterfactual digital twin $\hat{X}_{n,1:T_n}$, corresponding to the real patient record $X_{n,1:T_n}$, we need to identify the most closely matching patient record within $\tilde{X}_{k,1:T_k}$, where n is among T and k belongs to C . This step merges the unique personal traits of patient n with the temporal patterns observed in patient k , facilitating the creation of the synthetic pathway. We evaluate the applicability of TWIN-GPT trajectory generation by comparing the similarity between the synthesized trajectory and the most similar patient record.

4.2 Clinical Trial Outcome Prediction Evaluation of Digital Twins

To assess the practicality of digital twin models, we observe whether the additional synthetic data generated by models can successfully predict outcomes under different treatment modalities. Specifically, our experiments involve the following prediction tasks:

4.2.1 Dimension-wise probability.

To evaluate the similarity between twin data and the real data, we perform a dimensional-wise probability calculation. The calculation of dimension probabilities helps us to understand the probability of occurrence of each feature in the dataset, and it can provide quantitative metrics about the consistency and similarity between synthetic and real data. The Dimension-wise probability (DP) is calculated by

$$DP = \frac{V_f}{V_l}, \quad (6)$$

where V_f is the number of visits in the dataset containing a specific feature. V_l is the total number of accesses in the dataset. When digital twin models successfully produce synthetic data that closely mirrors the original, the distributional properties (DPs) of the synthetic data will approximate those of the real data. We calculate the Person correlation coefficient, $r \in [0, 1]$. If $r = 1$, it means that the model has high fidelity.

4.2.2 Counterfactual digital twin evaluation.

In the evaluation of counterfactual digital twins, for a specific patient, we identify the closest match from different treatment groups to act as a substitute for the inaccessible counterfactual outcomes, in line with established practices in causal inference research [60]. We assess the similarity between the digital twin and its corresponding record by calculating personalized Pearson correlation coefficients and quantify the fidelity by comparing data points between the synthetic and surrogate records.

4.2.3 Severe outcome prediction

To validate whether digital twin models can fully comprehend and replicate the underlying relationship between real-world data records and severe outcomes, we conducted severe outcome prediction validation. Firstly, we defined severe outcomes to include deaths and other critical clinical events. Then, we employed Long Short-Term Memory (LSTM) to forecast these severe outcomes. LSTM received real clinical data and synthetic data generated by different models for model training and prediction. Ultimately, we utilized the Area Under the Receiver Operating Characteristic Curve (AUROC) to assess the accuracy and performance of the predictions.

4.2.4 Adverse event prediction

Adverse event prediction is to show how much causal relation the synthetic data generated by digital twin models have maintained compared to the raw clinical data. We train another MLP (multiple-layer perceptron) to evaluate the prediction performance by inputting synthetic data and real data separately.

4.3 Digital Twins Clinical Privacy Evaluation

In the generation and utilization of synthetic data, privacy protection is of paramount importance. This section will delve into three primary methods of privacy risk evaluation: Presence Disclosure, Attribute Disclosure, and Nearest Neighbor Adversarial Accuracy Risk (NNAA).

4.3.1 Presence Disclosure

To evaluate the risk of privacy leakage, where an attacker analyzes synthetic data to infer whether the records of a particular individual participated in the training of the model, we employ sensitivity as a crucial metric. Sensitivity serves as an important indicator for assessing the privacy risk associated with synthetic data. By comprehending sensitivity, we can gain a clearer understanding of the level of privacy protection offered by synthetic data and implement appropriate measures to mitigate the risk of existential leakage. The sensitivity is calculated using the following formula:

$$S = \frac{R_k}{R_l}, \quad (7)$$

where R_k is the number of known records found in the synthetic data and R_l is the total number of known records. For instance, if we have 100 known records and detect 20 of them in the synthetic data, the sensitivity would be $20/100 = 0.2$. This implies a 20% probability for an attacker to confirm the presence of known samples in the training data. By calculating the sensitivity, we can determine the likelihood of an attacker identifying a known sample within the training data. If the synthetic data contains a limited number of known records, resulting in low sensitivity, it indicates a relatively secure nature of the synthetic data with a reduced risk of existential leakage. Conversely, if the synthetic data contains a substantial number of known records, leading to a high sensitivity, the risk of existential leakage becomes more pronounced.

4.3.2 Attribute Disclosure

Privacy leakage is when an attacker is able to obtain or infer sensitive information or unknown attributes of an individual, thereby violating an individual's right to privacy. Attribute leakage occurs when the attacker is able to infer other attributes of the patient based on a known subset of the data. To quantify this risk, we adopt average sensitivity as a metric. Average sensitivity measures the attacker's ability to infer unknown attributes. Mean sensitivity (MS) is calculated using the following formula:

$$MS = \frac{1}{N} \sum_{v=1}^N \frac{F_d}{F_l}, \quad (8)$$

where F_d represents the number of unknown features discovered, and F_l represents the total number of unknown features. For example, if an attacker knows ten attributes of a patient and can infer two unknown attributes from the synthetic data, the average sensitivity would be $2/10 = 0.2$. This implies that the attacker has a 20% probability of confirming the presence of these unknown attributes in the synthetic data. By computing the average sensitivity, we gain insight into the attacker's average capability to infer the patient's unknown attributes. A higher average sensitivity indicates a greater risk of privacy leakage, as it suggests that the attacker is more likely to infer unknown attributes. Conversely, a lower average sensitivity indicates a lower risk of privacy leakage, as it implies that the attacker's inference capability is relatively weak.

4.3.3 Nearest Neighbor Adversarial Accuracy Risk (NNAA)

NNAA is a measure of the degree to which a model overfits the original data, directly relating to privacy leakage risk. The NNAA risk score is calculated as follows:

$$\text{NNAA risk score} = AA_{ES} - AA_{TS}, \quad (9)$$

where AA_{ES} and AA_{TS} represent the aggregated distances between synthetic data and evaluation data, and between synthetic data and real data, respectively. They are calculated as follows:

$$AA_{ES} = \frac{1}{2} \left(\frac{1}{N} \sum_{i=1}^N 1(d_{ES}(i) > d_{EE}(i)) + \frac{1}{N} \sum_{i=1}^N 1(d_{SE}(i) > d_{SS}(i)) \right). \quad (10)$$

$$AA_{TS} = \frac{1}{2} \left(\frac{1}{N} \sum_{i=1}^N 1(d_{TS}(i) > d_{TT}(i)) + \frac{1}{N} \sum_{i=1}^N 1(d_{ST}(i) > d_{SS}(i)) \right). \quad (11)$$

Here, $d_{ES}(i)$, d_{TS} , d_{SE} and d_{EE} , d_{TT} , d_{SS} represent the nearest neighbor distances among synthetic data, evaluation data, and real data respectively. For example, if the average distance between synthetic data and evaluation data is greater than that between synthetic data and real data, the NNAA risk score will be positive, indicating potential over-fitting of the model to the training data, hence increasing the risk of privacy leakage.

Through these three methods, we can more comprehensively evaluate the privacy risks of synthetic data, thereby better protecting individual privacy.

5 EXPERIMENTS

5.1 Experimental Setup

5.1.1 Data source

Original clinical trial dataset: We trained TWIN-GPT using a Phase III breast cancer trial dataset (NCT00174655), analyzing Disease-Free Survival (DFS) across different treatment methods. The study randomly divided 2,887 patients into groups to compare the efficacy of docetaxel, either alone or with doxorubicin followed by CMF, against doxorubicin alone or combined with cyclophosphamide, then CMF, in patients with positive axillary lymph nodes. This dataset, publicly available in Project Data, facilitated our performance evaluation.

Trial Outcome Prediction (TOP) dataset: We also utilized the multi-modal TOP dataset [35] for predicting clinical trial outcomes. This dataset integrates clinical trial-related information from multiple data sources, with each trial record including drug molecule information, disease information, eligibility criteria, and trial result information. The dataset is divided into three phases: 1,160 Phase I trials, 4,449 Phase II trials, and 3,436 Phase III trials. The drug molecule information includes the names of candidate drugs and their functional groups. The disease information includes the ICD-10 codes, disease descriptions, and disease hierarchy represented by CCS codes. The eligibility criteria for the trials are described using unstructured natural language, including inclusion and exclusion criteria. The trial result information includes binary indicators for trial success (1) or failure (0), trial phase, start and end dates, trial sponsor, and trial scale (i.e., the number of participants).

5.1.2 Data preprocessing

We processed this dataset by extracting medications, treatments, and adverse events from the original clinical trial data. Then we selected the top 100 most frequently used medications and the top 50 most frequent adverse events, which contain most of the information in this dataset. We also merged all rare events (frequency < 50) into one additional adverse event, so that the model could fully utilize all samples. Regarding the TOP dataset [35], we utilized three distinct phases of this dataset to construct a twin network model. The study fully capitalized on the complete information available in the TOP dataset, wherein the criteria for trial qualification were delineated as background knowledge for establishing twin states, whereas the rest was considered clinical medical data for developing twin characteristics.

5.1.3 Baseline Models

We compare TWIN-GPT with the following baseline methods:

- **EVA [7]** utilizes variational autoencoders to create synthetic versions of electronic health records, serving as a generative model for this purpose.
- **SynTEG [82]** is a representative generative model that employs GANs to produce synthetic versions of EHRs. It uses transformer [66] as neural architecture in the dependency extraction part and Wasserstein GAN with gradient penalty (WGAN-GP) [3, 40] in the conditional generation part.
- **PromptEHR [72]** leverages real EHRs to train a prompt learning-based generative language model for synthetic EHR generation.
- **TWIN-VAE [30]** can detail clinical data through the development of individualized clinical trial digital twins, utilizing variational autoencoders (VAE) for this process.
- **k-NN-based method [6]** is a simple model that modifies the real patient data by picking random parts from its nearest neighbors.

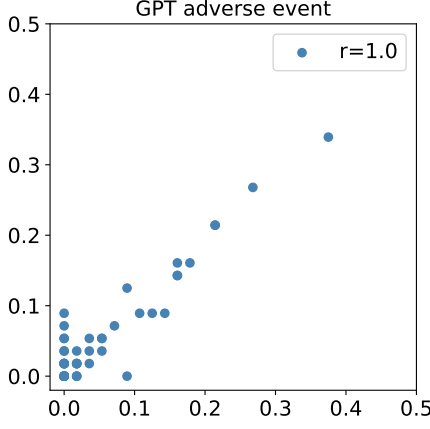


Figure 2: On the *Original clinical trial dataset*, we analyzed the dimension-wise Pearson correlation coefficient (r) of adverse events to evaluate the performance of TWIN-GPT. The x-axis displays the probability across dimensions for real data, while the y-axis signifies the probability associated with synthetic data.

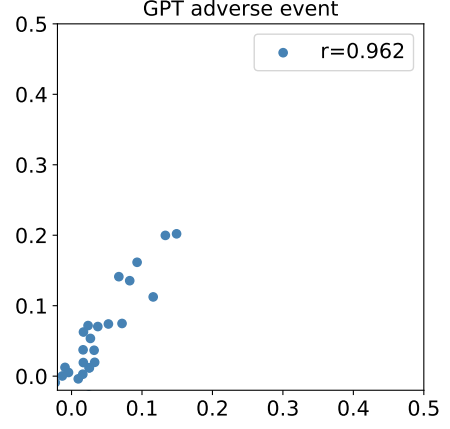


Figure 3: On the *TOP dataset*, we analyzed the dimension-wise Pearson correlation coefficient (r) of adverse events to evaluate the performance of TWIN-GPT. The x-axis displays the probability across dimensions for real data, while the y-axis is the probability associated with synthetic data.

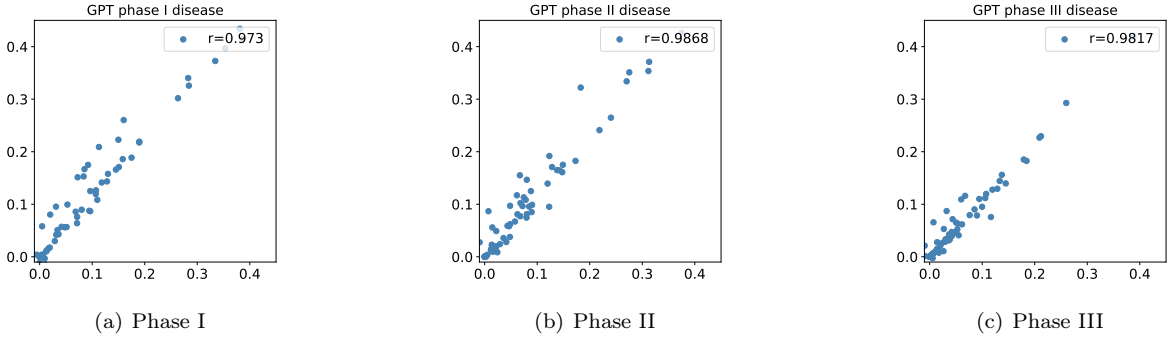


Figure 4: On the *TOP dataset*, we analyzed the dimension-wise Pearson correlation coefficient (r) of adverse events in the three phases to evaluate the performance of TWIN-GPT. The x-axis displays the probability across dimensions for real data, while the y-axis signifies the probability associated with synthetic data.

5.2 Generation Quality

5.2.1 Personalized Generation.

To make sure that TWIN-GPT has fully learned every dimension’s distribution precisely and accurately, we calculate all DPs of every adverse event separately from both real and generated synthetic data. Fig. 2 shows the performance of TWIN-GPT for Breast Cancer data. We compare the performance of dimensions’ distribution of TWIN-GPT and other baselines. The r s of adverse events for *EVA*, *SynTEG*, *PromptEHR*, *k-NN* and *TWIN-VAE* are -0.06, -0.07, 0.14, 1.0 and 0.99, respectively [30]. We can see that TWIN-GPT has higher fidelity than *SynTEG*, *PromptEHR*, and *TWIN-VAE*. Meanwhile, *k-NN* achieves performance comparable to TWIN-GPT, which can be easily explained that *k-NN* essentially copies and merges fragments from real data to generate synthetic data. However, *k-NN* cannot be used to generate EHR data directly because all the generated data can be linked to their original patient’s record, which will lead to the privacy risk of leaking information. Regarding the TOP dataset, we conducted overall DP calculations for the three medical phases in Fig. 3 and independent DPs calculations for the three clinical trial phases as shown in Fig. 4. In both scenarios, TWIN-GPT demonstrated high performance with $r \geq 0.96$. Since the TOP dataset is a multimodal dataset, the comparison algorithms used in the previous dataset do not apply to this dataset. Here, we used *k-NN* to calculate for the *TOP dataset*, where its r is 1, slightly higher than our TWIN-GPT. As mentioned before, *k-NN* is not suitable due to the potential for privacy risks associated with linking generated data back to the original patient records.

We also find out per-patient DPs to determine how well each synthetic record matches the associated synthetic

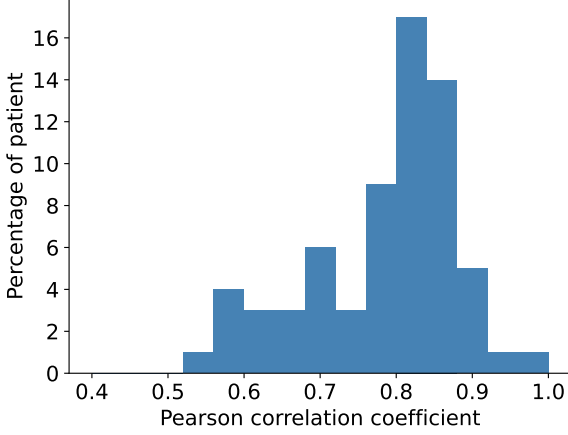


Figure 5: Patient-wise Pearson correlation coefficient (r) for TWIN-GPT. r is charting the distributional properties (DPs) of each patient’s closest match on the x-axis against the DPs of their respective synthetic digital twin on the y-axis. Most of the participants have high fidelity (r larger than 0.8).

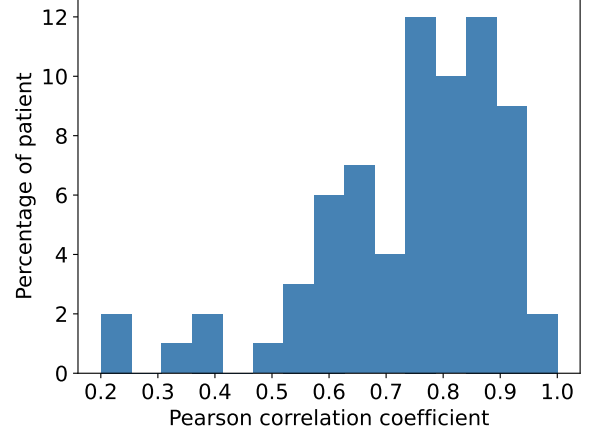


Figure 6: Counterfactual Generation (r) for TWIN-GPT. r is charting the distributional properties (DPs) of each patient’s closest match on the x-axis against the DPs of their respective synthetic digital twin on the y-axis. Most of the participants have high fidelity (r larger than 0.8).

record. We compute the Pearson Correlation Coefficient, r . The comparison of distributional properties (DPs) between synthetic and real data across all patients is analyzed through Pearson Correlation Coefficients, shown in a histogram within Fig. 5. This comparison indicates the synthetic data’s high fidelity on a feature-wise level, with a significant portion of correlation coefficients (r values) surpassing 0.8.

5.2.2 Counterfactual Generation.

To assess the quality of the counterfactual generation results, we train an LSTM model on real data to predict severe outcomes. Subsequently, we utilize this trained model to predict the counterfactual digital twins generated by TWIN-GPT, representing the simulated patients assigned to the alternative treatment arm. We then compare these predictions with the surrogate ground truth outcomes. Notably, the obtained AUROC score of 0.821, which is quite close to 0.838, AUROC score of the predictions with real data, demonstrates the high fidelity of the generated counterfactual digital twins.

Just like the way we determine the feature-wise fidelity in the *Personalized Generation* part, we assess the distributional properties (DPs) of actual data from the closest neighbor against the DPs of the corresponding synthetic data to determine the Pearson correlation coefficient (r). This comparison yields coefficients that are represented in Fig. 6. The results indicate that the digital twins of most patients exhibit a high degree of similarity to their real-life counterparts. These digital twins exhibit high r s that are larger than 0.8.

5.3 Digital Twins Clinical Trial Prediction

5.3.1 Severe outcome prediction

We train an LSTM to predict the severe outcome. This model takes in the real clinical data and synthetic data generated by TWIN-GPT. We show this severe outcome prediction result in Fig. 7. The LSTM achieves nearly the same AUROC scores when taking in the synthetic data generated by TWIN-GPT as taking in the real data, indicating that TWIN-GPT can fully understand and reproduce the latent relationship between records and severe outcomes in real data.

5.3.2 Adverse event prediction

This task is to see how much causal relation the synthetic data have maintained compared to the raw clinical data. We train an MLP to predict the adverse event at the next step by taking in real and synthetic data generated by different models separately. Results are shown in Fig. 8, where both TWIN-GPT and k -NN-based model have similar performance with the real data, indicating that our method captures the temporal causal relations accurately.

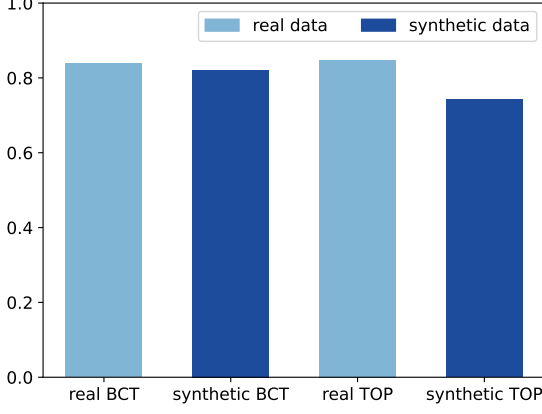


Figure 7: Severe outcome prediction results measured by AUROC scores. The AUROC scores of prediction made by LSTM when taking in real and synthetic data are quite close.

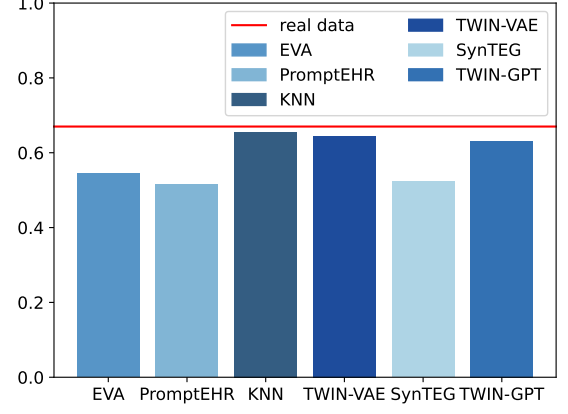


Figure 8: Adverse event prediction AUROC scores. The red line means the AUROC score of MLP to predict the adverse event by taking in real data. We can see that the synthetic data generated by TWIN-GPT and k -NN-based model have similar performance when the MLP predictor is trained on synthetic data and real data.

5.4 Digital Twins Clinical Privacy Protection

Privacy protection is of paramount importance in the generation and utilization of synthetic data. In this part, we evaluate three primary indexes: Presence Disclosure, Attribute Disclosure, and Nearest Neighbor Adversarial Risk (NNAA).

5.4.1 Presence Disclosure

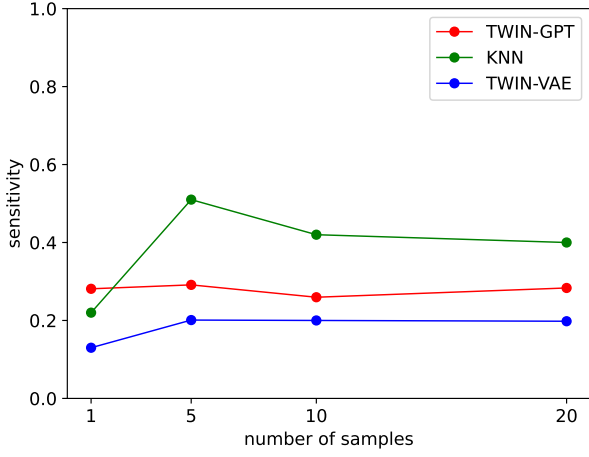
If an attacker finds that the synthetic data was trained by TWIN-GPT from the patient n 's record $X_{n;1:T_n}$, we call it presence disclosure. We assume that there are total $m\%$ of training data that had been known by the attackers and set m as 1%, 5%, 10%, and 20%. After calculating the sensitivity through Eq. 7, we display the result in Fig. 9(a). As the number of known samples rises, the sensitivity of TWIN-GPT has remained stable at around 20% (the attackers can recognize 20% of the real patients' records from synthetic data they know). Correspondingly, the k -NN-based method reaches the maximum sensitivity of around 50%. Additionally, we observe that in terms of presence disclosure, TWIN-GPT's sensitivity is slightly higher than that of TWIN-VAE but significantly lower than the k -NN algorithm. This could be because TWIN-GPT, as a large language model-based method, might possess a greater capability to capture and replicate the subtle differences of the training data. Such high fidelity in data replication may inadvertently lead to synthetic data retaining too many identifiable features of the original training data, thus increasing the risk of presence disclosure. However, on the *TOP dataset*, both the overall medical trial sensitivity for presence disclosure and the phase-by-phase medical trial sensitivity for presence disclosure are better than k -NN in Fig. 10.

5.4.2 Attribute Disclosure

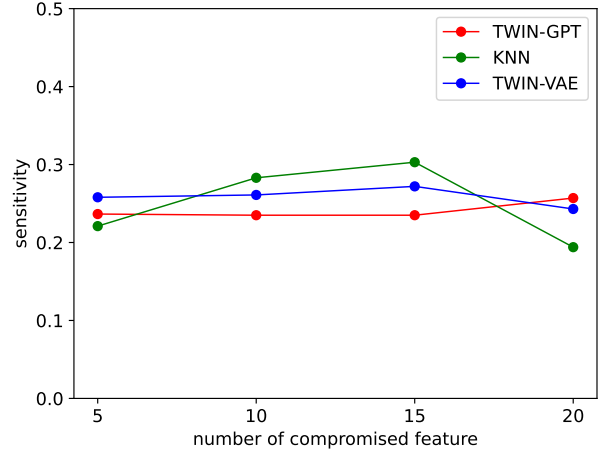
Here, we assume that the attackers know parts of the training set and have access to $x\%$ of features of the records. We set x as 1, 5, 10, and 20 in this experiment. When an attacker can infer additional attributes of an individual based on the features of a subset of the data he knows, the attribute disclosure occurs. We use Eq. 8 to calculate mean sensitivity. The results are shown in Fig. 9(b). We can see that the mean sensitivity of TWIN-GPT is generally less than the k -NN-based method and Twin method, meaning better performance. We can also observe that the maximum score of k -NN-based method and TWIN-GPT are respectively around 0.3 and 0.25. On the *TOP dataset*, as shown in Fig. 11, the mean sensitivity of TWIN-GPT is significantly lower than that of the k -NN algorithm. Across different numbers of features, TWIN-GPT's mean sensitivity is 0.2 percentage points lower than that of k -NN.

5.4.3 Nearest neighbor adversarial accuracy risk

NNAA is a measure of the degree to which a model overfits the original data, directly relating to privacy leakage risk. Here, we select 71 participants with 500 visit records as evaluation sets S_E . Correspondingly, we also choose 500 clinical records from real data as training sets S_T and from synthetic data to form S_S , like the method required.

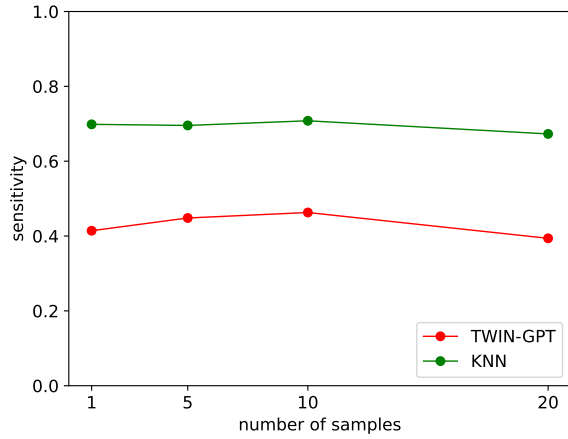


(a) Presence disclosure

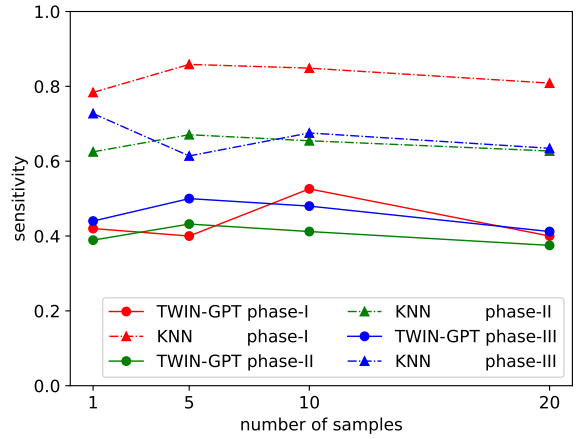


(b) Attribute disclosure

Figure 9: On the *Original clinical trial dataset*, Presence disclosure and Attribute disclosure sensitivity scores with a different number of samples known by the attacker. (Lower sensitivity is better).



(a) Presence disclosure: comprehensive perspective



(b) Presence disclosure: phase-by-phase analysis

Figure 10: On the *TOP dataset*, presence disclosure sensitivity scores with a different number of samples known by the attacker. Lower sensitivity is better.

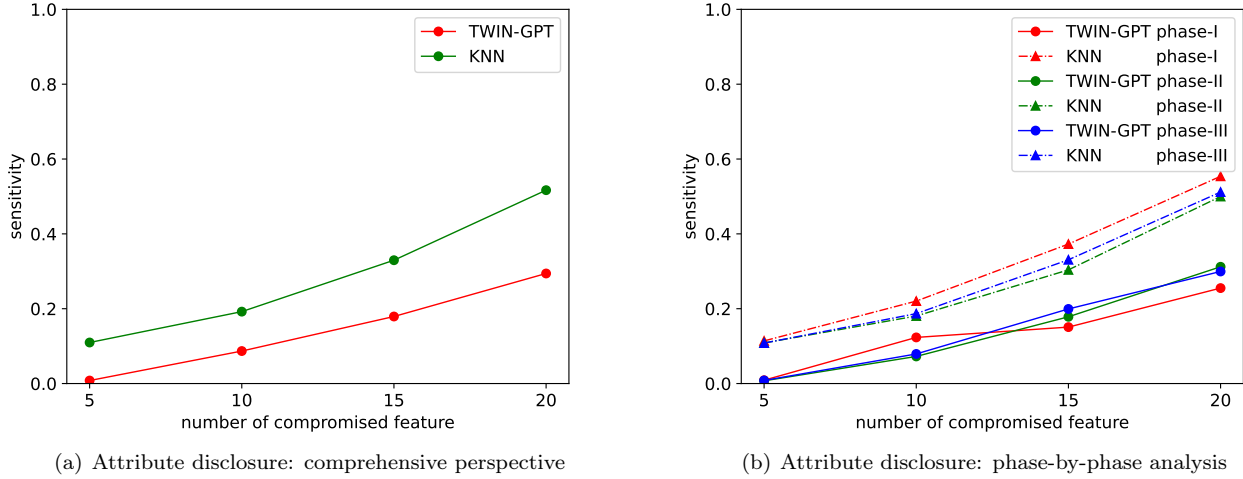


Figure 11: On the *TOP* dataset, Attribute disclosure sensitivity scores with a different number of samples known by the attacker. Lower sensitivity is better.

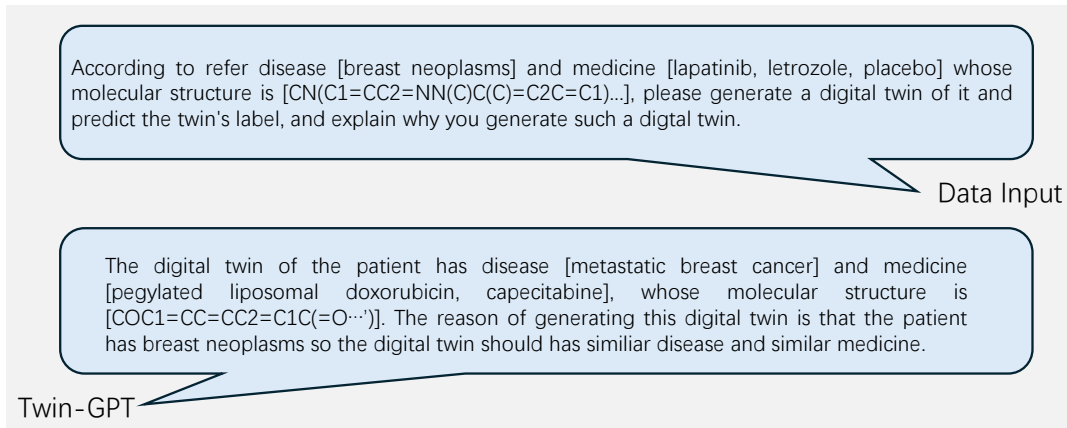


Figure 12: Explanation of TWIN-GPT.

TWIN-GPT achieves a score of 0.271. Generally, If the NNAA score is close to 0.5, we say that models overfit the original data. Therefore it suggests that TWIN-GPT is not excessively memorizing the original data and is instead learning more generalizable patterns.

5.5 Model Explainability

Unlike traditional models, our model functions as a “world model” endowed with a rich set of capabilities, enabling it to understand and interact with complex data landscapes. Therefore, our model possesses strong explainability. To this end, we conducted the explainability test of the twin generation results. As shown in Fig. 12, TWIN-GPT can provide explanations for its results when generating twins from input data.

5.6 Ablation Study

We compare the performance of TWIN-GPT before prompt fine-tuning and after prompt fine-tuning. We refer to the non-fine-tuned version as TWIN-GPT-*origin*. The accuracy of TWIN-GPT and TWIN-GPT-*origin* in severe outcome prediction is 0.821 and 0.537, respectively. Moreover, the attribute disclosure of TWIN-GPT when x set to 20 is less than 0.3, but in contrast, TWIN-GPT-*origin* reaches 0.530, meaning that attackers can easily infer additional attributes of an individual based on the features of a subset of the data he knows. In terms of the indicator of Personalized Generation quality and Counterfactual Generation quality, most of the participants’ r for TWIN-GPT are larger than 0.8, but the majority of participants’ r for TWIN-GPT-*origin* are less than 0.2.

Metric	TWIN-GPT	TWIN-GPT-origin
Accuracy in Severe Outcome Prediction	0.821	0.537
Attribute Disclosure when $x = 20$	0.260	0.530
Personalized Generation (r value)	0.812	0.121
Counterfactual Generation (r value)	0.785	0.310

Table 2: Ablation study of TWIN-GPT and TWIN-GPT-origin

6 CONCLUSIONS

In this paper, leveraging ChatGPT as the base model, we developed a specific large language model called **TWIN-GPT**, for generating personalized digital twins tailored for virtual clinical trial simulation. The approach proves advantageous for efficient and accurate prediction of clinical trial outcomes, particularly when confronted with limited EHR training data. The **TWIN-GPT** demonstrates exceptional performance, especially in terms of fidelity, utility, and privacy. The evaluation further validates that the **TWIN-GPT** can pose low privacy risks concerning presence disclosure, attribute disclosure, and nearest neighbor adversarial accuracy risks, effectively addressing privacy concerns inherent in traditional physical clinical trials.

References

- [1] Angier Allen, Anna Siefkas, Emily Pellegrini, Hoyt Burdick, Gina Barnes, Jacob Calvert, Qingqing Mao, and Ritankar Das. A digital twins machine learning model for forecasting disease progression in stroke patients. *Applied Sciences*, 11(12):5576, 2021.
- [2] Ali Amirahmadi, Mattias Ohlsson, and Kobra Etminani. Deep learning prediction models based on ehr trajectories: A systematic review. *Journal of biomedical informatics*, page 104430, 2023.
- [3] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International conference on machine learning*, pages 214–223. PMLR, 2017.
- [4] Taiyu Ban, Lyvzhou Chen, Xiangyu Wang, and Huanhuan Chen. From query tools to causal architects: Harnessing large language models for advanced causal discovery from data. *arXiv preprint arXiv:2306.16902*, 2023.
- [5] Mrinal Kanti Baowaly, Chia-Ching Lin, Chao-Lin Liu, and Kuan-Ta Chen. Synthesizing electronic health records using improved generative adversarial networks. *Journal of the American Medical Informatics Association*, 26(3):228–241, 2019.
- [6] Mandis Beigi, Afrah Shafquat, Jason Mezey, and Jacob W Aptekar. Synthetic clinical trial data while preserving subject-level privacy. In *NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research*, 2022.
- [7] Siddharth Biswal, Soumya Ghosh, Jon Duke, Bradley Malin, Walter Stewart, Cao Xiao, and Jimeng Sun. Eva: Generating longitudinal electronic health records using conditional variational autoencoders. In *Machine Learning for Healthcare Conference*, pages 260–282. PMLR, 2021.
- [8] Justin Brickell and Vitaly Shmatikov. The cost of privacy: destruction of data-mining utility in anonymized data publishing. In *Proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 70–78, 2008.
- [9] Maxime Cannesson, Ira Hofer, Joseph Rinehart, Christine Lee, Kathirvel Subramaniam, Pierre Baldi, Artur Dubrawski, and Michael R Pinsky. Machine learning of physiological waveforms and electronic health record data to predict, diagnose and treat haemodynamic instability in surgical patients: protocol for a retrospective study. *BMJ open*, 9(12):e031988, 2019.
- [10] Mengyuan Cao, Hang Wang, Xiaoming Liu, Jiahao Wu, and Mengting Zhao. Llm collaboration plm improves critical information extraction tasks in medical articles. In *China Health Information Processing Conference*, pages 178–185. Springer, 2023.
- [11] Giacomo Cappon, Martina Vettoretti, Giovanni Sparacino, Simone Del Favero, and Andrea Facchinetti. Replaybg: A digital twin-based methodology to identify a personalized model from type 1 diabetes data and simulate glucose concentrations to assess alternative therapies. *IEEE Transactions on Biomedical Engineering*, 2023.

- [12] Marco Cascella, Jonathan Montomoli, Valentina Bellini, and Elena Bignami. Evaluating the feasibility of chatgpt in healthcare: an analysis of multiple clinical and research scenarios. *Journal of medical systems*, 47(1):33, 2023.
- [13] Hung-Ching Chang, Antony M. Gitau, Siri Kothapalli, Danny R. Welch, Mihaela E. Sardi, and Matthew D. McCoy. Understanding the need for digital twins’ data in patient advocacy and forecasting oncology. *Frontiers in Artificial Intelligence*, 6, 2023.
- [14] Wenbing Chang, Yinglai Liu, Yiyong Xiao, Xinglong Yuan, Xingxing Xu, Siyue Zhang, and Shenghan Zhou. A machine-learning-based prediction method for hypertension outcomes based on medical data. *Diagnostics*, 9(4):178, 2019.
- [15] Anirban Chaudhuri, Graham Pash, David A Hormuth, Guillermo Lorenzo, Michael Kapteyn, Chengyue Wu, Ernesto ABF Lima, Thomas E Yankeelov, Karen Willcox, et al. Predictive digital twin for optimizing patient-specific radiotherapy regimens under uncertainty in high-grade gliomas. *Frontiers in Artificial Intelligence*, 6, 2023.
- [16] Zhengping Che, Yu Cheng, Shuangfei Zhai, Zhaonan Sun, and Yan Liu. Boosting deep learning risk prediction with generative adversarial networks for electronic health records. In *2017 IEEE International Conference on Data Mining (ICDM)*, pages 787–792. IEEE, 2017.
- [17] Jintai Chen, Shuai Huang, Ying Zhang, Qing Chang, Yixiao Zhang, Dantong Li, Jia Qiu, Lianting Hu, Xiaoting Peng, Yunmei Du, et al. Congenital heart disease detection by pediatric electrocardiogram based deep learning integrated with human concepts. *Nature Communications*, 15(1):976, 2024.
- [18] Jintai Chen, Kuanlun Liao, Kun Wei, Haochao Ying, Danny Z Chen, and Jian Wu. ME-GAN: Learning panoptic electrocardio representations for multi-view ECG synthesis conditioned on heart diseases. In *International Conference on Machine Learning*, pages 3360–3370. PMLR, 2022.
- [19] Jintai Chen, Jiahuan Yan, Qiyuan Chen, Danny Ziyi Chen, Jian Wu, and Jimeng Sun. Excelformer: Can a dnn be a sure bet for tabular prediction? In *KDD*, 2024.
- [20] Jintai Chen, Bohan Yu, Biwen Lei, Ruiwei Feng, Danny Z Chen, and Jian Wu. Doctor imitator: A graph-based bone age assessment framework using hand radiographs. In *Medical Image Computing and Computer Assisted Intervention–MICCAI 2020: 23rd International Conference, Lima, Peru, October 4–8, 2020, Proceedings, Part VI 23*, pages 764–774. Springer, 2020.
- [21] Jintai Chen, Xiangshang Zheng, Hongyun Yu, Danny Z Chen, and Jian Wu. Electrocardio panorama: synthesizing new ECG views with self-supervision. *arXiv preprint arXiv:2105.06293*, 2021.
- [22] Tianyi Chen, Nan Hao, Yingzhou Lu, and Capucine Van Rechem. Uncertainty quantification on clinical trial outcome prediction. *arXiv preprint arXiv:2401.03482*, 2024.
- [23] Travers Ching, Daniel S Himmelstein, Brett K Beaulieu-Jones, Alexandr A Kalinin, Brian T Do, Gregory P Way, Enrico Ferrero, Paul-Michael Agapow, Michael Zietz, Michael M Hoffman, et al. Opportunities and obstacles for deep learning in biology and medicine. *Journal of The Royal Society Interface*, 15(141):20170387, 2018.
- [24] Edward Choi, Mohammad Taha Bahadori, Andy Schuetz, Walter F Stewart, and Jimeng Sun. Doctor ai: Predicting clinical events via recurrent neural networks. In *Machine learning for healthcare conference*, pages 301–318. PMLR, 2016.
- [25] Edward Choi, Siddharth Biswal, Bradley Malin, Jon Duke, Walter F Stewart, and Jimeng Sun. Generating multi-label discrete patient records using generative adversarial networks. In *Machine learning for healthcare conference*, pages 286–305. PMLR, 2017.
- [26] Edward Choi, Andy Schuetz, Walter F Stewart, and Jimeng Sun. Using recurrent neural network models for early detection of heart failure onset. *Journal of the American Medical Informatics Association*, 24(2):361–370, 2017.
- [27] Jiebin Chu, Wei Dong, Jinliang Wang, Kunlun He, and Zhengxing Huang. Treatment effect prediction with adversarial deep learning using electronic health records. *BMC Medical Informatics and Decision Making*, 20:1–14, 2020.
- [28] Jan Clusmann, Fiona R Kolbinger, Hannah Sophie Muti, Zunamys I Carrero, Jan-Niklas Eckardt, Narmin Ghaffari Laleh, Chiara Maria Lavinia Löffler, Sophie-Caroline Schwarzkopf, Michaela Unger, Gregory P Veldhuizen, et al. The future landscape of large language models in medicine. *Communications medicine*, 3(1):141, 2023.

- [29] Genevieve Coorey, Gemma A Figtree, David F Fletcher, Victoria J Snelson, Stephen Thomas Vernon, David Winlaw, Stuart M Grieve, Alistair McEwan, Jean Yee Hwa Yang, Pierre Qian, et al. The health digital twin to tackle cardiovascular disease—a review of an emerging interdisciplinary field. *NPJ digital medicine*, 5(1):126, 2022.
- [30] Trisha Das, Zifeng Wang, and Jimeng Sun. Twin: Personalized clinical trial digital twin generation. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining*, pages 402–413, 2023.
- [31] Cynthia Dwork and Rebecca Pottenger. Toward practicing privacy. *Journal of the American Medical Informatics Association*, 20(1):102–108, 2013.
- [32] Cristóbal Esteban, Stephanie L Hyland, and Gunnar Rätsch. Real-valued (medical) time series generation with recurrent conditional gans. *arXiv preprint arXiv:1706.02633*, 2017.
- [33] Scott L Fleming, Alejandro Lozano, William J Haberkorn, Jenelle A Jindal, Eduardo Reis, Rahul Thapa, Louis Blankemeier, Julian Z Genkins, Ethan Steinberg, Ashwin Nayak, et al. Medalign: A clinician-generated dataset for instruction following with electronic medical records. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, pages 22021–22030, 2024.
- [34] Tianfan Fu, Wenhao Gao, Connor Coley, and Jimeng Sun. Reinforced genetic algorithm for structure-based drug design. *Advances in Neural Information Processing Systems*, 35:12325–12338, 2022.
- [35] Tianfan Fu, Kexin Huang, and Jimeng Sun. Automated prediction of clinical trial outcome, February 2 2023. US Patent App. 17/749,065.
- [36] Tianfan Fu, Kexin Huang, Cao Xiao, Lucas M Glass, and Jimeng Sun. Hint: Hierarchical interaction network for clinical-trial-outcome predictions. *Patterns*, 3(4), 2022.
- [37] Tianfan Fu, Cao Xiao, Xinhao Li, Lucas M Glass, and Jimeng Sun. Mimosa: Multi-constraint molecule sampling for molecule optimization. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 35, pages 125–133, 2021.
- [38] Benjamin CM Fung, Ke Wang, Rui Chen, and Philip S Yu. Privacy-preserving data publishing: A survey of recent developments. *ACM Computing Surveys (Csur)*, 42(4):1–53, 2010.
- [39] Sagar Goyal, Eti Rastogi, Sree Prasanna Rajagopal, Dong Yuan, Fen Zhao, Jai Chintagunta, Gautam Naik, and Jeff Ward. Healai: A healthcare llm for effective medical documentation. In *Proceedings of the 17th ACM International Conference on Web Search and Data Mining*, pages 1167–1168, 2024.
- [40] Ishaan Gulrajani, Faruk Ahmed, Martin Arjovsky, Vincent Dumoulin, and Aaron C Courville. Improved training of wasserstein gans. *Advances in neural information processing systems*, 30, 2017.
- [41] Mehak Gupta, Thao-Ly T Phan, H Timothy Bunnell, and Rahmatollah Beheshti. Obesity prediction with ehr data: A deep learning approach with interpretable elements. *ACM Transactions on Computing for Healthcare (HEALTH)*, 3(3):1–19, 2022.
- [42] Soheil Hassanipour, Haleh Ghaem, Morteza Arab-Zozani, Mozhgan Seif, Mohammad Fararouei, Elham Abdzadeh, Golnar Sabetian, and Shahram Paydar. Comparison of artificial neural network and logistic regression models for prediction of outcomes in trauma patients: A systematic review and meta-analysis. *Injury*, 50(2):244–250, 2019.
- [43] Tilda Herrgårdh, Elizabeth Hunter, Kajsa Tunedal, Håkan Öрман, Julia Amann, Francisco Abad Navarro, Catalina Martinez-Costa, John D Kelleher, and Gunnar Cedersund. Digital twins and hybrid modelling for simulation of physiological variables and stroke risk. *bioRxiv*, pages 2022–03, 2022.
- [44] Hanyao Huang, Ou Zheng, Dongdong Wang, Jiayi Yin, Zijin Wang, Shengxuan Ding, Heng Yin, Chuan Xu, Renjie Yang, Qian Zheng, et al. Chatgpt for shaping the future of dentistry: the potential of multi-modal large language model. *International Journal of Oral Science*, 15(1):29, 2023.
- [45] Peter B Jensen, Lars J Jensen, and Søren Brunak. Mining electronic health records: towards better research applications and clinical care. *Nature Reviews Genetics*, 13(6):395–405, 2012.
- [46] Hye Jin Kam and Ha Young Kim. Learning representations for the early detection of sepsis with deep neural networks. *Computers in biology and medicine*, 89:248–255, 2017.
- [47] Mert Karabacak and Konstantinos Margetis. Embracing large language models for medical applications: opportunities and challenges. *Cureus*, 15(5), 2023.

- [48] Ying Liu, Lin Zhang, Yuan Yang, Longfei Zhou, Lei Ren, Fei Wang, Rong Liu, Zhibo Pang, and M Jamal Deen. A novel cloud-based framework for the elderly healthcare services using digital twin. *IEEE access*, 7:49088–49101, 2019.
- [49] Yingzhou Lu, Yi-Tan Chang, Eric P Hoffman, Guoqiang Yu, David M Herrington, Robert Clarke, Chiung-Ting Wu, Lulu Chen, and Yue Wang. Integrated identification of disease specific pathways using multi-omics data. *bioRxiv*, page 666065, 2019.
- [50] Yingzhou Lu, Tianyi Chen, Nan Hao, Capucine Van Rechem, Jintai Chen, and Tianfan Fu. Uncertainty quantification and interpretability for clinical trial approval prediction. *Health Data Science*, 2024.
- [51] Yingzhou Lu, Minjie Shen, Huazheng Wang, Xiao Wang, Capucine van Rechem, and Wenqi Wei. Machine learning for synthetic data generation: a review. *arXiv preprint arXiv:2302.04062*, 2023.
- [52] Sewon Min, Xinxu Lyu, Ari Holtzman, Mikel Artetxe, Mike Lewis, Hannaneh Hajishirzi, and Luke Zettlemoyer. Rethinking the role of demonstrations: What makes in-context learning work? *arXiv preprint arXiv:2202.12837*, 2022.
- [53] Harsha Nori, Nicholas King, Scott Mayer McKinney, Dean Carignan, and Eric Horvitz. Capabilities of gpt-4 on medical challenge problems. *arXiv preprint arXiv:2303.13375*, 2023.
- [54] Yujin Oh, Sangjoon Park, Hwa Kyung Byun, Jin Sung Kim, and Jong Chul Ye. Llm-driven multimodal target volume contouring in radiation oncology. *arXiv preprint arXiv:2311.01908*, 2023.
- [55] OpenAI. Chatgpt. <https://openai.com/blog/chatgpt/>, 2022.
- [56] Cheng Peng, Xi Yang, Kaleb E Smith, Zehao Yu, Aokun Chen, Jiang Bian, and Yonghui Wu. Model tuning or prompt tuning? a study of large language models for clinical concept and relation extraction. *Journal of Biomedical Informatics*, page 104630, 2024.
- [57] Alvin Rajkomar, Eyal Oren, Kai Chen, Andrew M Dai, Nissan Hajaj, Michaela Hardt, Peter J Liu, Xiaobing Liu, Jake Marcus, Mimi Sun, et al. Scalable and accurate deep learning with electronic health records. *NPJ digital medicine*, 1(1):1–10, 2018.
- [58] Kan Ren, Jiarui Qin, Lei Zheng, Zhengyu Yang, Weinan Zhang, Lin Qiu, and Yong Yu. Deep recurrent survival analysis. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 4798–4805, 2019.
- [59] Divya Saxena and Jiannong Cao. Generative adversarial networks (gans) challenges, solutions, and future directions. *ACM Computing Surveys (CSUR)*, 54(3):1–42, 2021.
- [60] Uri Shalit, Fredrik D Johansson, and David Sontag. Estimating individual treatment effect: generalization bounds and algorithms. In *International conference on machine learning*, pages 3076–3085. PMLR, 2017.
- [61] Minjie Shen, Yue Zhao, Chenhao Li, Fan Meng, Xiao Wang, David Herrington, Yue Wang, Tim Fu, and Capucine Van Rechem. Genocraft: A comprehensive, user-friendly web-based platform for high-throughput omics data analysis and visualization. *arXiv preprint arXiv:2312.14249*, 2023.
- [62] Wenqi Shi, Ran Xu, Yuchen Zhuang, Yue Yu, Jieyu Zhang, Hang Wu, Yuanda Zhu, Joyce Ho, Carl Yang, and May D Wang. Ehragent: Code empowers large language models for complex tabular reasoning on electronic health records. *arXiv preprint arXiv:2401.07128*, 2024.
- [63] Ting Fang Tan, Kabilan Elangovan, Liyuan Jin, Yao Jie, Li Yong, Joshua Lim, Stanley Poh, Wei Yan Ng, Daniel Lim, Yuhe Ke, et al. Fine-tuning large language model (llm) artificial intelligence chatbots in ophthalmology and llm-based evaluation using gpt-4. *arXiv preprint arXiv:2402.10083*, 2024.
- [64] Arun James Thirunavukarasu, Darren Shu Jeng Ting, Kabilan Elangovan, Laura Gutierrez, Ting Fang Tan, and Daniel Shu Wei Ting. Large language models in medicine. *Nature medicine*, 29(8):1930–1940, 2023.
- [65] Alexandre Vallée. Digital twin for healthcare systems. *Frontiers in Digital Health*, 5, 2023.
- [66] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. *Advances in neural information processing systems*, 30, 2017.
- [67] Rohit Venugopal, Noman Shafqat, Ishwar Venugopal, Benjamin Mark John Tillbury, Harry Demetrios Stafford, and Aikaterini Bourazeri. Privacy preserving generative adversarial networks to model electronic health records. *Neural Networks*, 153:339–348, 2022.

- [68] Ethan Waisberg, Joshua Ong, Mouayad Masalkhi, and Andrew G Lee. Large language model (llm)-driven chatbots for neuro-ophthalmic medical education. *Eye*, pages 1–3, 2023.
- [69] Junda Wang, Zhichao Yang, Zonghai Yao, and Hong Yu. Jmlr: Joint medical llm and retrieval training for enhancing reasoning and professional question answering capability. *arXiv preprint arXiv:2402.17887*, 2024.
- [70] Wenjie Wang, Pengfei Tang, Jian Lou, Yuanming Shao, Lance Waller, Yi-an Ko, and Li Xiong. Igamt: Privacy-preserving electronic health record synthesization with heterogeneity and irregularity. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 38, pages 15634–15643, 2024.
- [71] Yubo Wang, Xueguang Ma, and Wenhui Chen. Augmenting black-box llms with medical textbooks for clinical question answering. *arXiv preprint arXiv:2309.02233*, 2023.
- [72] Zifeng Wang and Jimeng Sun. Promptehr: Conditional electronic healthcare records generation with prompt learning, 2022.
- [73] Chengyan Wu, Zehong Lin, Wenlong Fang, and Yuyan Huang. A medical diagnostic assistant based on llm. In *China Health Information Processing Conference*, pages 135–147. Springer, 2023.
- [74] Alexandre Yahi, Rami Vanguri, Noémie Elhadad, and Nicholas P Tatonetti. Generative adversarial networks for electronic health records: A framework for exploring and evaluating methods for predicting drug-induced laboratory test trajectories. *arXiv preprint arXiv:1712.00164*, 2017.
- [75] Jiahuan Yan, Jintai Chen, Chaowen Hu, Bo Zheng, Yaojun Hu, Jimeng Sun, and Jian Wu. SERVAL: Synergy learning between vertical models and LLMs towards oracle-level zero-shot medical prediction. *arXiv preprint arXiv:2403.01570*, 2024.
- [76] Jiahuan Yan, Haojun Gao, Zhang Kai, Weize Liu, Danny Chen, Jian Wu, and Jintai Chen. Text2Tree: Aligning text representation to the label tree hierarchy for imbalanced medical classification. In *EMNLP-Findings*, 2023.
- [77] Jiahuan Yan, Bo Zheng, Hongxia Xu, Yiheng Zhu, Danny Chen, Jimeng Sun, Jian Wu, and Jintai Chen. Making pre-trained language models great on tabular prediction. In *ICLR*, 2024.
- [78] Thomas E Yankeelov, David A Hormuth, Ernesto ABF Lima, Guillermo Lorenzo, Chengyue Wu, Lois C Okereke, Gaiane M Rauch, Aradhana M Venkatesan, and Caroline Chung. Designing clinical trials for patients who are not average. *Iscience*, 27(1), 2024.
- [79] Jinsung Yoon, Michel Mizrahi, Nahid Farhady Ghalaty, Thomas Jarvinen, Ashwin S Ravi, Peter Brune, Fanyu Kong, Dave Anderson, George Lee, Arie Meir, et al. Ehr-safe: generating high-fidelity and privacy-preserving synthetic electronic health records. *NPJ Digital Medicine*, 6(1):141, 2023.
- [80] Dong Yuan, Eti Rastogi, Gautam Naik, Jai Chintagunta, Sree Prasanna Rajagopal, Fen Zhao, Sagar Goyal, and Jeff Ward. A continued pretrained llm approach for automatic medical note generation. *arXiv preprint arXiv:2403.09057*, 2024.
- [81] Chi Zhang, Hadi Fanaee-T, and Magne Thoresen. Feature extraction from unequal length heterogeneous ehr time series via dynamic time warping and tensor decomposition. *Data Mining and Knowledge Discovery*, 35(4):1760–1784, 2021.
- [82] Ziqi Zhang, Chao Yan, Thomas A Lasko, Jimeng Sun, and Bradley A Malin. Synteg: a framework for temporal structured electronic health data simulation. *Journal of the American Medical Informatics Association*, 28(3):596–604, 2021.
- [83] Wayne Xin Zhao, Kun Zhou, Junyi Li, Tianyi Tang, Xiaolei Wang, Yupeng Hou, Yingqian Min, Beichen Zhang, Junjie Zhang, Zican Dong, et al. A survey of large language models. *arXiv preprint arXiv:2303.18223*, 2023.
- [84] Xiang Zhong, Farnaz Babaie Sarijaloo, Aditya Prakash, Jaeyoung Park, Chanyan Huang, Amelia Barwise, Vitaly Herasevich, Ognjen Gajic, Brian Pickering, and Yue Dong. A multidisciplinary approach to the development of digital twin models of critical care delivery in intensive care units. *International Journal of Production Research*, 60(13):4197–4213, 2022.