

Tutorial

Integration of Federated Learning and Blockchain in Health Care: Tutorial on Medical Data, Architectures, Privacy, Security, and Regulatory Compliance

Yahya Shahsavari¹, PhD; Yaser Baseri¹, PhD; Abdelhakim Hafid¹, PhD; Oussama Abderrahmane Dambri², PhD; Dimitrios Makrakis², PhD

¹Department of Computer Science and Operations Research, Université de Montréal, Montréal, QC, Canada

²School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, ON, Canada

Corresponding Author:

Yahya Shahsavari, PhD
Department of Computer Science and Operations Research
Université de Montréal
2900 Bd Édouard-Montpetit
Montréal, QC H3T 1J4
Canada
Phone: 1 5144514964
Email: yahya.shahsavari@etsmtl.ca

Abstract

The convergence of artificial intelligence (AI), blockchain technology, and health care represents one of the most transformative yet technically challenging frontiers in computational medicine. As health care systems adopt data-driven paradigms for precision medicine and clinical decision support, the need for secure, privacy-preserving, and collaborative learning frameworks has become critical. This tutorial introduces a comprehensive, clinically oriented, and compliance-aware framework integrating federated learning (FL) and blockchain for secure and privacy-preserving health care analytics. FL enables collaborative training across distributed institutions without raw data sharing, in alignment with privacy regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). However, FL remains vulnerable to model poisoning and gradient leakage. To address these risks, we introduce blockchain-based FL (BCFL), which leverages blockchain's immutable ledger and decentralized consensus to enhance trust, verifiability, and auditability. The tutorial's main contributions include (1) a taxonomy of diverse medical data types and their FL requirements; (2) three integration architectures (fully coupled, semicoupled, and loosely coupled) analyzed for security, scalability, and regulatory compliance; (3) a security analysis of health care-specific vulnerabilities and mitigation strategies using advanced cryptography, such as zero-knowledge proofs, homomorphic encryption, and differential privacy; and (4) a regulatory compliance framework addressing HIPAA, GDPR, and United States Food and Drug Administration guidelines for AI-enabled medical devices. We demonstrate BCFL's relevance across major health care applications, including disease prediction, medical imaging, patient monitoring, and drug discovery, and highlight emerging research directions such as quantum-resilient cryptography, scalable interoperability, and automated compliance. This tutorial serves as a foundational resource for advancing secure, compliant, and collaborative AI in health care; fostering privacy-preserving analytics; and improving patient outcomes.

J Med Internet Res 2026;28:e80178; doi: [10.2196/80178](https://doi.org/10.2196/80178)

Keywords: blockchain technology; health care security; medical data privacy; IoT health care; machine learning; HIPAA compliance

Introduction

Background

The convergence of artificial intelligence (AI), blockchain technology, and health care represents one of the most transformative yet technically challenging frontiers in computational medicine. As health care systems worldwide transition toward data-driven paradigms for precision medicine, clinical decision support, and population health management, the exponential growth in medical data generation—from electronic health records (EHRs) and medical imaging to genomic sequencing and Internet of Things (IoT)-enabled continuous monitoring—presents unprecedented opportunities for advancing health care through machine learning (ML) [1-3].

Federated learning (FL) has emerged as a promising paradigm for collaborative model training across distributed health care institutions while maintaining data locality [4, 5]. However, standard FL architectures face challenges, including model poisoning, gradient leakage, and coordination failures [6-8]. Blockchain technology offers complementary capabilities through immutable audit trails, decentralized trust, and automated smart contract execution [9], yet integration with FL in health care introduces unique scalability, efficiency, and regulatory compliance challenges.

This tutorial addresses a critical gap by providing a structured, cross-disciplinary framework that integrates blockchain with FL in the context of health care, with explicit coverage of medical data taxonomies, clinical workflows, and regulatory compliance.

While prior surveys have explored the integration of FL and blockchain applications in health care and beyond [10-13], this tutorial differs in scope and emphasis. In particular, we provide (1) a systematic medical data taxonomy that classifies diverse health care data types (EHRs, imaging, genomics, biometrics, Internet of Medical Things [IoMT], clinical trials, etc) and analyzes their specific FL requirements; (2) a set of three integration architectures (fully coupled, semicoupled, and loosely coupled) with detailed evaluation of security, scalability, and compliance tradeoffs tailored to health care deployments; (3) comprehensive treatment of advanced cryptographic defenses (zero-knowledge proofs [ZKPs], homomorphic encryption [HE], and differential privacy [DP]) with health care-specific vulnerability analysis; and (4) a structured regulatory compliance framework mapping Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and United States Food and Drug Administration (FDA) guidelines to blockchain-FL system design. Moreover, while prior surveys have typically focused on high-level concepts, our tutorial adopts a more comprehensive and tutorial-oriented scope by combining blockchain fundamentals, FL methodologies, health care-specific applications, security analysis, and forward-looking research directions. This extensive focus allows us to introduce a comprehensive, clinically oriented, and compliance-aware framework that integrates FL and blockchain for health care, providing actionable insights for both researchers and practitioners implementing secure, privacy-preserving, and regulation-compliant collaborative analytics systems. Table 1 contrasts this tutorial with earlier blockchain-based FL (BCFL) surveys and frameworks to clarify the contributions.

Table 1. Comparison of our tutorial with prior work on the integration of blockchain and federated learning in health care.

Reference	Medical data taxonomy	Integration architecture	Cryptography and privacy	Regulatory compliance
Abbas et al [10]	General overview	No specific architecture	Privacy mechanisms	Limited overview
Cheng et al [11]	Partial coverage	No specific architecture	Basic techniques	GDPR ^a
Ngoupayou Limbepe et al [12]	Limited scope	No specific architecture	Basic techniques	HIPAA ^b and GDPR
Myrzashova et al [13]	Not included	No specific architecture	Security analysis	Not addressed
This paper	Comprehensive taxonomy	Three distinct architectures	Security and privacy analysis	HIPAA, GDPR, and FDA ^c

^aGDPR: General Data Protection Regulation.

^bHIPAA: Health Insurance Portability and Accountability Act.

^cFDA: Food and Drug Administration.

Motivation and Problem Statement

Contemporary health care faces a fundamental paradox: the increasing need for large-scale, collaborative data analytics to advance medical knowledge is juxtaposed with stringent privacy regulations and the inherent sensitivity of medical data. Traditional centralized approaches to health care ML create critical vulnerabilities where patient information aggregated in single repositories becomes an attractive target for sophisticated attacks [14,15]. Recent breaches affecting millions of patient records underscore the inadequacy of current security models, particularly when regulatory frameworks, such as HIPAA and GDPR, and emerging

national data protection laws impose severe penalties for data mishandling [16].

While FL addresses data locality concerns by enabling distributed model training, it introduces health care-critical vulnerabilities. Model poisoning attacks could compromise diagnostic accuracy [6,7], potentially leading to misdiagnosis or incorrect treatment recommendations. Gradient leakage exploits can enable patient reidentification from shared model updates [8,17], violating privacy guarantees that health care institutions must maintain. Coordination failures in distributed learning processes could disrupt critical clinical workflows [18], affecting real-time decision support systems.

Blockchain technology addresses these vulnerabilities through immutable audit trails that ensure accountability, decentralized trust establishment that eliminates single points of failure, automated smart contract execution for verifiable protocol compliance, and comprehensive data provenance tracking [9]. However, health care-specific integration challenges remain, including scalability constraints when processing high-frequency medical data updates from IoMT devices, energy efficiency requirements for sustainable long-term deployment in resource-constrained clinical environments, compliance with medical device regulations for AI/ML systems, and real-time performance requirements for clinical decision support applications.

Existing BCFL approaches [19-23] are predominantly designed for generic data types and fail to address health care-specific requirements. Critical gaps include a lack of regulatory compliance frameworks for HIPAA and GDPR, insufficient integration with clinical workflows and existing health IT systems, inadequate support for multimodal medical data with heterogeneous privacy requirements, and absence of explainability mechanisms required for medical decision-making. This tutorial fills these gaps by providing a comprehensive framework tailored specifically for health care applications.

Contributions and Novelty

This tutorial advances the state-of-the-art at the intersection of blockchain technology, FL, and health care informatics through several methodological and theoretical contributions:

1. Comprehensive medical data taxonomy for FL: We develop a systematic classification of medical data types (EHRs, imaging, genomics, biometrics, IoT sensors, clinical trials, etc) and their specific requirements for FL implementations, including privacy sensitivity levels, regulatory considerations, and technical constraints for distributed processing.
2. Novel integration architecture framework: We introduce and formally define 3 distinct BCFL integration architectures (fully coupled, semicoupled, and loosely coupled) specifically designed for health care environments, with detailed analysis of their security guarantees, scalability characteristics, and regulatory compliance capabilities.
3. Health care-specific security and privacy analysis: We provide a comprehensive security analysis of BCFL systems in health care contexts, identifying unique vulnerabilities related to medical data sensitivity, regulatory requirements, and clinical workflow dependencies, along with corresponding mitigation strategies.
4. Regulatory compliance framework: We systematically examine how BCFL architectures can satisfy complex health care regulations (HIPAA, GDPR, and FDA guidelines for AI/ML-based medical devices),

providing practical guidance for implementation in real-world health care settings.

5. Research roadmap and future directions: We identify critical research gaps at the intersection of blockchain, FL, and health care, proposing specific research directions that could accelerate adoption and address current technical limitations.

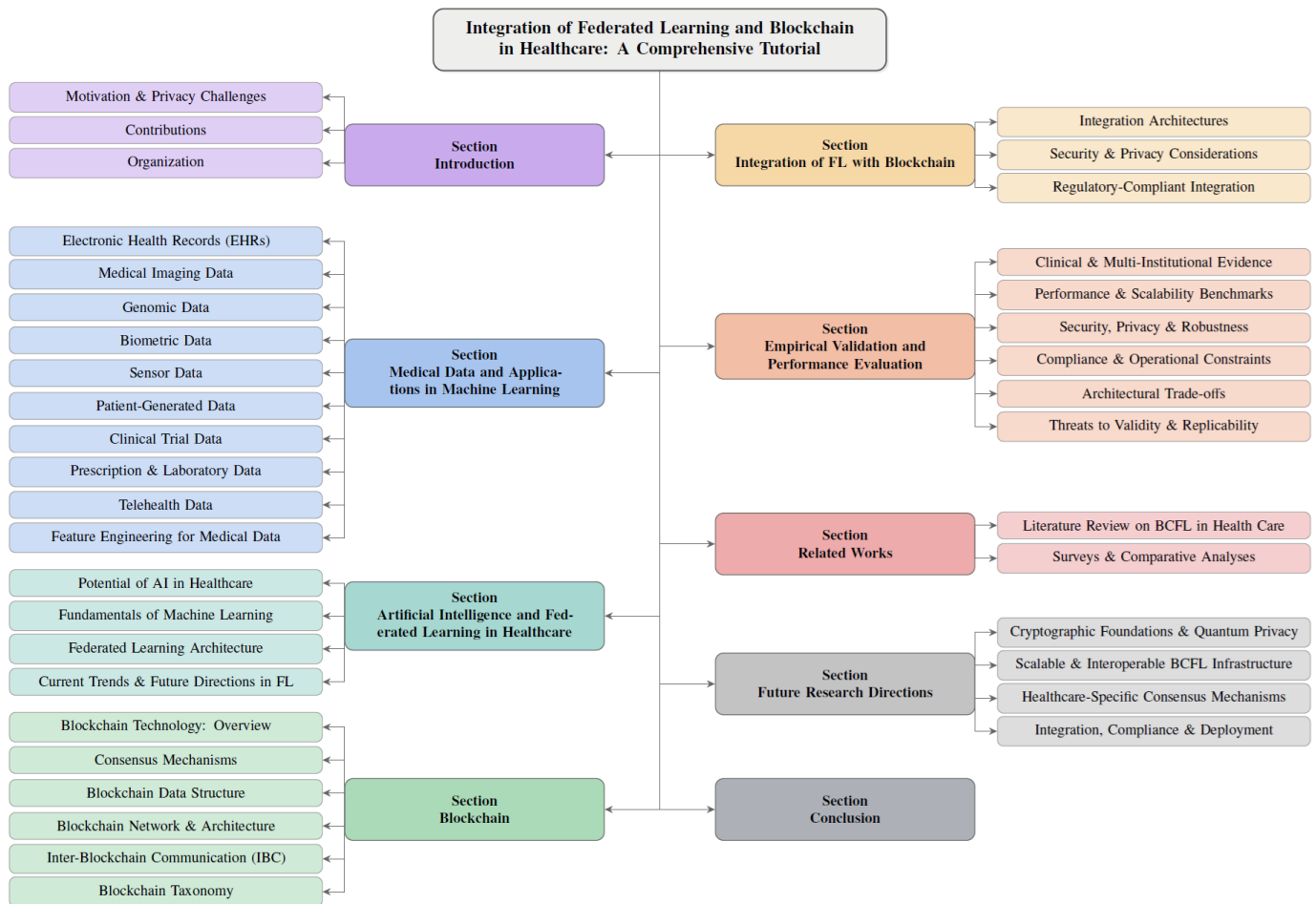
Tutorial Scope and Target Audience

This tutorial is designed for researchers and practitioners at the intersection of health care informatics, distributed systems, and ML. Our target audience includes (1) health care informaticians seeking to implement privacy-preserving collaborative analytics, (2) computer scientists developing secure FL systems, (3) blockchain researchers exploring health care applications, (4) clinical researchers interested in multi-institutional collaborations, and (5) regulatory and policy experts working on health care data governance. The tutorial assumes familiarity with basic ML concepts but provides a comprehensive background on FL and blockchain technologies. We emphasize practical implementation considerations while maintaining rigorous technical depth appropriate for publication in top-tier venues.

Organization

The remainder of this tutorial is structured as illustrated in [Figure 1](#). The Medical Data and Applications in ML section introduces a comprehensive taxonomy of medical data types, including EHRs, imaging, genomics, and sensor data, and discusses their relevance to ML. The AI and FL in Health Care section explores the evolution of AI in health care, highlighting FL paradigms, their challenges, and future trends. The Blockchain section reviews fundamental blockchain concepts, such as consensus, data structures, and cross-chain communication, with a focus on health care applicability. The Integration of FL With Blockchain section presents integration architectures that combine FL and blockchain, along with their security, privacy, and regulatory implications in health care. The Empirical Validation and Performance Evaluation section synthesizes quantitative evidence from clinical deployments, benchmarks, and adversarial robustness studies to provide empirical validation, assess performance tradeoffs, and establish the framework's real-world feasibility. The Related Work section offers a critical review of previous work on the integration of blockchain and FL to contextualize the contributions of this tutorial. The Future Research Directions section synthesizes emerging research challenges and opportunities, grouped under cryptographic resilience, infrastructure scalability, health care-specific consensus and incentives, and regulatory compliance in system integration. Finally, the Conclusion section summarizes the key findings and reflects on the real-world translation of BCFL systems into clinical practice.

Figure 1. Organizational structure of the tutorial.



Medical Data and Applications in ML

Overview

Medical data encompass a diverse array of information crucial for understanding, diagnosing, and treating various health conditions. These data, ranging from patient demographics and medical history to diagnostic images and genomic sequences, hold immense potential for advancing health care through ML applications. By harnessing the power of ML algorithms, medical data can be analyzed to extract valuable insights, predict patient outcomes, personalize treatments, and optimize health care delivery. However, the utilization of medical data for ML requires careful consideration of data storage and management practices to ensure compliance with privacy regulations, maintain data integrity, and facilitate seamless access for research and clinical purposes. This section explores the different types of medical data and their applications in ML.

EHR Data

EHRs are digital patient charts containing medical history, diagnoses, medications, treatment plans, immunization dates, allergy information, medical images, and lab results, providing a comprehensive, up-to-date view for informed decision-making [24,25]. The key EHR features include the following: (1) *digital format*, electronic records replace paper

for easier storage, access, and sharing; (2) *interoperability*, designed for sharing among different providers and organizations, facilitating better care coordination; (3) *real-time access*, authorized professionals get quick access to critical information, which is crucial for emergencies; (4) *patient engagement*, features allow patients to access data, schedule appointments, and communicate with providers; (5) *decision support*, tools offer alerts for drug interactions, screening reminders, and clinical guidelines; and (6) *data security and privacy*, security measures protect confidentiality, with access restricted to authorized personnel [26]. EHRs are a rich source of structured and unstructured data for ML applications. ML algorithms analyze this comprehensive patient information to extract insights, predict outcomes, identify patterns, and improve clinical decision-making [27,28]. In ML, EHR data are used for tasks, including the following: (1) *predictive analytics*, where models forecast medical events (eg, hospital readmission, disease onset, and mortality) for proactive, personalized care [29,30]; (2) *disease identification and diagnosis*, where algorithms assist in early detection by identifying subtle patterns and anomalies, aiding accurate and timely diagnoses [31,32]; and (3) *treatment recommendations*, where models suggest personalized plans based on history, demographics, genetics, and past responses to optimize outcomes [33].

Medical Imaging Data

Medical imaging data encompass diverse visual representations of internal body structures, acquired via distinct imaging modalities [34,35] for clinical scrutiny, diagnosis, and ongoing assessment. The key components of medical imaging data are (1) patient information, (2) imaging modalities, (3) image files, and (4) reports. First, patient information includes basic demographic and identifying details (eg, name, ID, age, and gender). Second, among imaging modalities, each modality uses specific physical principles [36] to generate images adapted to clinical needs. The imaging modalities include (1) radiography for projection imaging of osseous structures [37]; (2) computed tomography (CT) for high-resolution cross-sectional imaging using x-ray and computational reconstruction [38]; (3) magnetic resonance imaging (MRI) for detailed soft tissue visualization via magnetic fields and radiofrequency pulses [39]; (4) ultrasonography for real-time acoustic wave imaging, which is ideal for soft tissues and dynamic processes [40]; (5) nuclear medicine imaging for visualizing organ function via radiopharmaceuticals [41]; (6) positron emission tomography for quantitative functional imaging, especially in oncology, neurology, and cardiology [42]; and (7) fluoroscopic imaging for dynamic, real-time x-ray visualization during interventional and functional studies [43]. Third, regarding image files, medical data, including metadata (patient information, acquisition parameters, and image details) [44], are stored, shared, and transmitted according to technical standards [45], notably Digital Imaging and Communications in Medicine (DICOM) [46]. Fourth, reports include narrative documents generated by radiologists summarizing image analysis findings for the treatment planning of referring physicians. Medical imaging data have a wide range of ML applications in health care [47], including the following: (1) *disease diagnosis and classification*, ML algorithms assist in the diagnosis and classification of diseases like cancer and neurological, cardiovascular, and musculoskeletal disorders [48]; (2) *computer-aided detection*, computer-aided detection systems use ML to help radiologists detect abnormalities (eg, tumors, lesions, and fractures), improving diagnostic accuracy and efficiency [49]; (3) *image-based biomarker discovery*, ML identifies imaging biomarkers associated with diseases or treatment responses, which is valuable for prognosis, efficacy assessment, and personalized medicine [50,51]; (4) *treatment planning and monitoring*, imaging data are used to develop personalized plans, and ML predicts outcomes, monitors progression, and optimizes treatment strategies [52]; (5) *image reconstruction and enhancement*, ML techniques (eg, deep learning) improve image quality from various modalities (MRI, CT, and ultrasonography) by reducing artifacts and enhancing resolution for better interpretation [53]; (6) *image registration and fusion*, ML algorithms automatically align and combine multiple images (from different modalities or time points) for comprehensive visualization and analysis; and (7) *drug discovery and development*, ML analyzes imaging data to evaluate drug effects on disease progression, identify potential drug targets, and optimize delivery methods [54].

Genomic Data

Genomic data pertain to information concerning the organization and operation of the genome within an organism [55,56]. In health care ML, this refers to comprehensive information from an individual's genome (entire DNA/genetic composition), offering profound insights into genetic predispositions, treatment responses, and overall health [57]. The key components for medical use cases include the following: (1) *genome sequences*, the complete set of genetic material (DNA), consisting of nucleotides (A, T, C, and G) that encode genetic information; (2) *genes*, specific DNA sequences that encode instructions for protein synthesis, including their location, structure, and function; (3) *single nucleotide polymorphisms*, single-nucleotide variations that can influence traits, disease susceptibility, and drug responses, along with their associated phenotypic and disease information [58]; (4) *copy number variations*, genomic alterations involving changes in the number of copies of DNA segments, affecting gene dosage and leading to phenotypic variations and disease susceptibility [59]; (5) *gene expression profiles*, information on the activity levels of different genes (often generated via microarrays or RNA sequencing [60]), providing insights into protein synthesis; (6) *epigenetic modifications*, heritable changes in gene expression (eg, DNA methylation and histone modifications) that do not alter the DNA sequence but influence gene activity and phenotype [61]; and (7) *genetic variation databases*, compilations of genomic data, genetic variants, annotations, and associated phenotypic information from various sources (eg, population studies and disease databases) [62]. These components are essential for understanding the genetic basis of diseases, identifying risk factors, and developing personalized health care approaches. The utilization of genomic data in health care ML includes the following: (1) *disease prediction and risk stratification*, ML algorithms scrutinize genomic data to discern patterns and variations linked to specific diseases, assessing associated health risks [63]; (2) *personalized medicine*, genomic data form the basis for personalized treatment plans [64,65], and ML models predict individual medication responses for tailored strategies [66-68]; (3) *drug discovery and computational genomics*, ML analyzes genomic data to expedite discovery, identifying drug targets and comprehending genetic underpinnings for more efficacious therapeutic solutions [69]; (4) *genomic counseling*, ML algorithms decipher complex genomic data, assisting health care professionals in communicating intricate genetic details, risks, and familial implications [70]; (5) *early detection and diagnostics*, integrating genomic data and ML algorithms facilitates early detection by discerning subtle genetic variations indicative of specific conditions, enabling timely intervention [71,72]; (6) *research and population health informatics*, aggregated genomic data subjected to ML can advance the understanding of disease genetic foundations at the population level, informing public health initiatives and epidemiological studies [73]; and (7) *genomic sequencing and computational analysis*, ML plays a crucial role in interpreting extensive genomic datasets from sequencing

technologies, identifying genetic mutations, variations, and other health-impacting information [74].

Biometric Data

Biometric data in the medical context refer to unique physical or behavioral characteristics used for individual identification and monitoring. These data are crucial in health care for patient identification, medical record access control, personalized treatments, and health condition monitoring. The components of biometric data include the following: (1) *physiological biometrics*, data types like fingerprints, facial recognition, iris/retina scans, DNA, smell recognition, and hand geometry data [75]; (2) *behavioral biometrics*, data types such as voice recognition, gait analysis, and typing dynamics data [75]; (3) *health-related biometrics*, data types such as heart rate, blood pressure, blood oxygen levels, electrocardiography (ECG) patterns [76], and brain wave patterns (electroencephalography [EEG] patterns) [77]; and (4) *analytical biometric technologies*, advanced modalities like microbial biometrics, which analyze unique microbiome compositions for identification and health assessment [78], and olfactory biometrics, which utilize distinctive body odor profiles for identification and disease detection [79].

Biometric data integrated into health care ML encompass quantifiable physiological or behavioral attributes [75,80] for accurate identification [81,82], secure access [83,84], and health assessment [85]. The primary applications of biometric data in health care ML include the following: (1) *biometric identification and access control*, biometric features (eg, fingerprints and facial characteristics) are pivotal for precise identification and heightened security, governing access to sensitive areas, EHRs, and medical devices [80, 86]; (2) *patient identification and record matching*, biometric identifiers (eg, fingerprints and iris scans) ensure precise linkage of patients to their health records, minimizing errors, with ML algorithms enhancing matching accuracy and elevating care quality [87-90]; (3) *biometric monitoring for health assessment*, continuous monitoring of biometric data (eg, heart rate and ECG data) via wearables/sensors facilitates real-time health assessment, and ML analyzes dynamic data for the early detection of anomalies, supporting timely intervention and personalized management [91-93]; (4) *behavioral biometrics for mental health monitoring*, behavioral biometrics (eg, typing and voice modulation) contribute to assessing mental health and detecting behavioral changes [94,95], and ML models discern patterns indicative of conditions, aiding targeted interventions [96]; (5) *biometric data in clinical trials*, biometric data are used for participant identification, monitoring, and data integrity, and ML assists in efficient management and analysis, ensuring study validity [97,98]; (6) *voice and speech analysis for diagnostics*, ML algorithms process voice patterns to detect potential markers for conditions like Parkinson disease [99,100] or respiratory disorders [101,102], contributing to diagnostic capabilities [103]; and (7) *facial recognition for patient monitoring*, facial recognition is used for monitoring patient well-being and distress, and ML analyzes facial expressions, offering insights into comfort levels and enhancing care quality [104,105].

Sensor Data

Sensor data in medical contexts represent information collected from various devices (wearable, implantable, or environmental devices) to monitor health, detect condition changes, and assist diagnoses. These data continuously track physiological parameters, activity levels, and environmental conditions. The components of medical sensor data include the following: (1) *wearable sensors*, data from devices like heart rate monitors, blood pressure monitors, blood glucose monitors, activity trackers, and pulse oximeters; (2) *implantable sensors*, data from devices like cardiac monitors, glucose monitors, and intraocular pressure sensors; (3) *environmental sensors*, data gathered from air quality monitors (for pollutants and allergens affecting respiratory conditions) and temperature/humidity sensors; (4) *specialized medical sensors*, data from ECG, EEG, electromyography, gait sensors, and sleep monitors; and (5) *smart health homes*, data extracted from fall detectors and bed sensors that monitor sleep patterns, bed occupancy, and vital signs.

Sensor data used in health care ML are collected from various sources (wearables, medical equipment, and monitoring tools) [106,107], providing real-time health and activity insights. ML algorithms analyze these data to make predictions, identify patterns, and offer personalized insights. The utilization of sensor data in health care ML includes the following: (1) vital sign monitoring, (2) wearable devices for activity tracking, (3) blood glucose monitoring and continuous glucose monitoring, (4) ECG monitoring, (5) sleep monitoring, (6) environmental sensors, (7) medication adherence monitoring, (8) fall detection and activity recognition, and (9) biometric sensors for stress and emotion monitoring. First, in vital sign monitoring, ML analyzes continuous vital sign data (heart rate, blood pressure, etc) to detect anomalies, predict health deteriorations, and offer early warnings [108,109]. Second, regarding wearable devices for activity tracking, ML models analyze data from accelerometers and gyroscopes to assess physical health, detect abnormalities, and provide personalized insights for fitness and rehabilitation [110]. Third, in blood glucose monitoring and continuous glucose monitoring, ML algorithms analyze continuous glucose monitoring data to predict glucose level trends, recommend insulin dosages, and enhance diabetes management [111]. Fourth, in ECG monitoring, ML interprets ECG data to identify cardiac abnormalities, predict cardiovascular risk, and recommend early interventions [112, 113]. Fifth, in sleep monitoring, ML algorithms analyze sleep data (from wearables and bed sensors) to identify disorders, provide insights into sleep hygiene, and recommend personalized interventions [114,115]. Sixth, regarding environmental sensors, ML correlates environmental data (air quality and temperature) with health outcomes, aiding in identifying triggers for respiratory conditions or allergies [116]. Seventh, in medication adherence monitoring, ML analyzes adherence patterns tracked by smart sensors, sending reminders and providing providers with compliance insights [117,118]. Eighth, regarding fall detection and activity recognition, ML models use motion sensor data for fall risk assessment, accident prediction, and adapting care plans for

individuals with mobility challenges [119]. Ninth, regarding biometric sensors for stress and emotion monitoring, ML analyzes biometric signals (eg, skin conductance and heart rate variability) to provide insights into mental health, stress management, and emotional well-being [120,121].

Patient-Generated Data

Patient-generated data (PGD) in health care ML refer to health-related information actively contributed by patients [122,123], distinct from traditional clinical records. Sourced directly via wearables, mobile apps, and patient-reported outcomes (PROs), PGD foster a patient-centric, data-driven approach, enabling personalized interventions, early detection, and improved patient-provider communication [124]. Beyond sensor data, PGD utilization in health care ML includes the following: (1) *mobile health apps and surveys*, patients input health information and feedback via apps, and ML processes these data to derive insights into treatment effectiveness, medication adherence, and satisfaction, informing personalized care plans [125]; (2) *social media and online communities*, patients share health experiences and concerns online [126], and ML conducts analyses on social media data for health-related trends, sentiment, and public health monitoring, contributing to population health research and patient perspectives [127,128]; (3) *genomic and genetic data sharing*, patients voluntarily contribute genetic information for research, and ML analyzes aggregated genomic data to identify genetic factors associated with diseases, fostering precision medicine advancements [129]; and (4) *telehealth and virtual visits*, patients offer health updates during virtual consultations, and ML algorithms analyze PGD from these visits to support clinical decision-making, monitor treatment progress, and enhance virtual health care quality [130].

Clinical Trial Data

Clinical trial data refer to information systematically collected during trials designed to evaluate the safety, efficacy, or effectiveness of new medical interventions (drugs, devices, and procedures) in human participants [131]. These data, governed by a structured protocol, inform medical decision-making, regulatory approvals, and medical knowledge advancements. Integrating these data into ML models enables the development of predictive algorithms, risk assessment tools, and decision support systems, contributing to evidence-based medicine, personalized treatments, and enhanced clinical research efficiency [132]. The key components of clinical trial data are as follows: (1) demographic information, (2) informed consent, (3) medical history, (4) intervention details, (5) clinical assessments, (6) adverse events, (7) efficacy endpoints, (8) follow-up data, and (9) protocol deviations. First, demographic information includes details on study participants (age, gender, race, and ethnicity) incorporated into ML models to assess intervention response across groups and develop personalized treatment plans. Second, informed consent involves documentation confirming that participants were informed of risks/benefits and voluntarily agreed to participate, ensuring ethical standards and regulatory compliance, with ML incorporating this to restrict

the analysis to consented data [133,134]. Third, medical history includes information on pre-existing conditions, relevant history, and concurrent medications, which is used to identify comorbidities that may impact treatment outcomes. Fourth, intervention details include specifics about the product/procedure (dosage, administration, and protocol), with ML analyzing these details to identify patterns associated with treatment success or failure, predicting efficacy in future cases [135]. Fifth, clinical assessments include physical examinations, lab tests, imaging, and measurements to assess the health status and intervention response, with ML processing this information to identify trends, correlations, or anomalies indicative of treatment responses or adverse events, aiding early detection and prediction [136]. Sixth, adverse events involve records of side effects experienced, including severity and relation to the intervention, with ML learning from these historical data to predict the likelihood of adverse events for new interventions, supporting risk assessment and proactive management [137,138]. Seventh, efficacy endpoints include measurements (eg, symptom relief and disease marker improvement) used to determine intervention effectiveness, with ML analyzing these data to develop predictive models for treatment success/failure and identify key contributing factors. Eighth, follow-up data include information on long-term outcomes, adherence, and sustained effects collected during posttrial visits, which is essential for longitudinal analyses, with ML using this information to predict the long-term effects of interventions, including sustained efficacy or potential relapse [139]. Ninth, protocol deviations involve documentation of deviations from the original plan and their reasons, with ML analyzing the data to identify how deviations impact study outcomes, allowing for adjustment or prediction of their potential effects [140].

Prescription and Medication Data

Prescription and medication data in medical records relate to prescribed drugs, dosage, frequency, and related details. These data are crucial for patient safety, medication management, monitoring public health and treatment efficacy, research, regulatory compliance, and facilitating communication. Integrated into EHRs, they provide a comprehensive medication history, allowing health care professionals to make informed decisions and avoid potential adverse events. Aggregated and anonymized data are used in research to broadly assess medication safety and effectiveness. The key components of prescription and medication data are as follows: (1) patient information; (2) prescriber information; (3) prescription date; (4) medication name; (5) dosage, frequency, and route of administration; (6) duration of treatment; (7) instructions for use; (8) refill information; (9) allergies and contraindications; (10) adverse reactions; (11) medication changes; (12) medication discontinuation; and (13) medication administration records (MARs). First, patient information includes identification details (name, date of birth, and demographics), which are used in ML for personalized treatment. Second, prescriber information includes details about the prescribing provider, with ML models being trained to recognize prescribing practices associated with positive patient outcomes [141]. Third, prescription date is the

date the prescription was issued, and temporal analysis assists in predicting medication adherence and treatment outcomes, with ML identifying patterns related to issuance timing and patient behavior [142]. Fourth, medication name involves generic and brand names, with ML models categorizing medications by therapeutic class, aiding in identifying commonalities in treatment outcomes [143]. Fifth, dosage, frequency, and route of administration include the prescribed amount/strength, how often it should be taken, and the administration method, which are crucial details for predicting adherence and adverse events, with ML models identifying optimal regimens [144]. Sixth, duration of treatment is the prescribed period, with ML models analyzing this to predict long-term outcomes, including treatment success and potential drug resistance [145]. Seventh, instructions for use include additional guidance (eg, taken with food and specific times), with natural language processing (NLP) approaches extracting insights from free-text instructions to identify nuances in patient guidance [146]. Eighth, refill information includes details on authorized refills, which are essential for predicting adherence and persistence, with ML identifying factors influencing refill behavior and predicting discontinuation likelihood [147]. Ninth, allergies and contraindications involve records of known patient allergies or contraindications, with ML identifying associations among these records, adverse drug reactions, and specific medications to predict safety and suitability for individual patients [148]. Tenth, adverse reactions involve documentation of experienced side effects, with data being analyzed to develop predictive models identifying patients at higher risk for specific side effects, enabling proactive management. Eleventh, medication changes include information about dosage adjustments or switches, with ML analyzing historical changes to predict future treatment modifications, assisting in personalized planning [129,149]. Twelfth, medication discontinuation involves the reason and date of stopping medication, with ML models predicting factors contributing to discontinuation, helping providers intervene to improve adherence [150]. Thirteenth, MARs include records of actual medication administration in a health care setting, with MAR data being used to train ML models for predicting administration patterns and identifying deviations from the prescribed regimen [151].

Laboratory Data

Laboratory data in medical records are the results of tests and analyses conducted on patient samples, which are essential for diagnosing, monitoring, and managing various medical conditions. The types of data collected vary by patient presentation and provider assessment. ML techniques (supervised, unsupervised, and deep learning) are applied depending on the nature of the data and analysis goals. The common types of laboratory data are the results of the following tests: (1) blood tests, (2) urinalysis, (3) microbiology tests, (4) pathology tests, (5) hematology tests, (6) immunology tests, (7) endocrine tests, (8) serology tests, (9) genetic tests, and (10) radiology and imaging studies. First, blood tests include assessments of the complete blood count (cell counts), blood chemistry panel (electrolytes,

glucose, and organ function tests), and lipid profile, with ML models identifying patterns in complete blood count results associated with specific diseases (eg, anemia and infections) [152]. Second, urinalysis involves examination of the physical/chemical properties of urine, with ML algorithms detecting patterns indicative of kidney disorders, urinary tract infections, or diabetes [153]. Third, microbiology tests involve identifying microorganisms and their antibiotic sensitivity, with ML assisting in microorganism identification from culture data and predicting antibiotic susceptibility for personalized treatment [154,155]. Fourth, pathology tests include tissue biopsy and cytology (cell examination) performed for disease/abnormality diagnosis (eg, cancer), with image recognition ML models trained on pathology slides assisting in identifying abnormal tissue or cancerous cells [50,156]. Fifth, hematology tests include coagulation studies (blood clotting) and erythrocyte sedimentation rate (an inflammation measure), with ML models analyzing coagulation data to predict the risk of bleeding or clotting disorders [157]. Sixth, immunology tests include antibody tests (detecting immune system antibodies) and viral load (measuring the virus in blood), with ML algorithms identifying patterns in antibody levels to diagnose autoimmune or infectious conditions [158,159]. Seventh, endocrine tests include assessments of hormone levels (eg, thyroid and insulin), with ML models analyzing these levels to predict and monitor endocrine disorders like thyroid dysfunction or diabetes [160,161]. Eighth, serology tests include analyses of serum components (proteins, enzymes, and electrolytes), with ML identifying markers associated with specific diseases, aiding early detection and monitoring [158]. Ninth, genetic tests involve the identification of specific genetic markers for condition diagnosis, with ML analyzing these data to identify disease risk, predict treatment response, or diagnose genetic disorders [70]. Tenth, radiology and imaging studies include diagnostic tests contributing to medical data, with image recognition/segmentation ML models being trained on radiology images to assist in diagnosing conditions like tumors or fractures.

Telehealth Data

Telehealth data refer to information collected during remote health care interactions between patients and providers [162]. These data are crucial in modern health care, utilizing technology (video, phone, and online platforms) to deliver services remotely and contributing to the overall patient record [163]. The key components of telehealth data are as follows: (1) audio and video recordings, (2) text-based communication, (3) diagnostic and monitoring device data, (4) EHR integration, (5) appointment and scheduling data, (6) patient demographics and consent, (7) prescription and medication data, and (8) PROs. First, audio and video recordings include recordings of virtual consultations used for documentation and quality assurance, with ML analyzing these for sentiment or clinical insights, speech recognition transcribing audio for verbal analysis, and facial recognition/sentiment analysis assessing patient emotions and engagement [164]. Second, text-based communication involves chat logs, texts, or emails containing symptom and

treatment information, with NLP extracting and categorizing information (symptoms and treatment discussions) and sentiment analysis gauging patient satisfaction and well-being [165]. Third, diagnostic and monitoring device data include data from remote devices (eg, blood pressure monitors, glucose meters, and wearables) that enable continuous remote health monitoring, with ML models analyzing trends and patterns, and time series analysis and predictive modeling detecting trends/anomalies in vital signs and predicting exacerbations of chronic conditions [166,167]. Fourth, EHR integration involves integration into EHRs/electronic medical records for a comprehensive patient view, with ML analyzing combined data to identify correlations between in-person and virtual interactions, improving diagnosis and treatment planning. Fifth, appointment and scheduling data include information on scheduling, duration, and attendance, with analysis optimizing appointment availability and patient access, and predictive analytics optimizing scheduling and resource allocation by anticipating demand. Sixth, patient demographics and consent include details about the patient and consent for services, ensuring privacy compliance and personalized care context, with ML analyzing demographic data for population health trends, targeted interventions, and service personalization. Seventh, prescription and medication data include information on prescriptions, management, and adherence, supporting virtual refills, with predictive modeling analyzing adherence patterns to inform personalized interventions and identifying medication-related risks and interactions [168]. Eighth, PROs include patient-reported data on symptoms, well-being, and effectiveness, with ML analyzing PROs via text mining and sentiment analysis to predict treatment responses and assess correlations with clinical outcomes to inform decisions [169].

Feature Engineering for Medical Data

While raw medical data provide the foundation for downstream ML applications, they often require substantial

transformation to become analytically useful. Feature engineering refers to the process of extracting, selecting, and constructing meaningful features from raw data to enhance model accuracy, interpretability, and generalizability [170]. This step is particularly critical in the health care domain due to the inherent heterogeneity, noise, and sparsity of clinical data.

The feature engineering process encompasses several essential techniques tailored to different data modalities. Normalization and encoding transform categorical variables and scale numerical values to comparable ranges. Temporal aggregation captures time-dependent patterns from longitudinal records such as EHR data. NLP embedding methods convert unstructured clinical notes into dense vector representations. Signal processing techniques extract meaningful patterns from physiological sensors and medical imaging. Dimensionality reduction methods address the curse of dimensionality while preserving informative variance in high-dimensional genomic or imaging data.

Effective feature engineering not only improves model performance but also enhances interpretability and supports reproducibility across diverse health care settings [171]. In FL scenarios, harmonizing feature spaces across distributed clients is crucial to ensure compatible model training and aggregation [171]. Figure 2 illustrates a high-level pipeline that uses systematic preprocessing transformations for mapping heterogeneous raw medical data (detailed taxonomy in Figure 3) to structured feature vectors suitable for downstream ML and FL modeling.

Figure 2. Feature engineering pipeline for heterogeneous medical data. Raw health care data from 10 diverse sources (detailed taxonomy in Figure 3) undergo systematic preprocessing and transformation to generate unified feature vectors for downstream machine learning (ML) or federated learning (FL) applications. NLP: natural language processing.

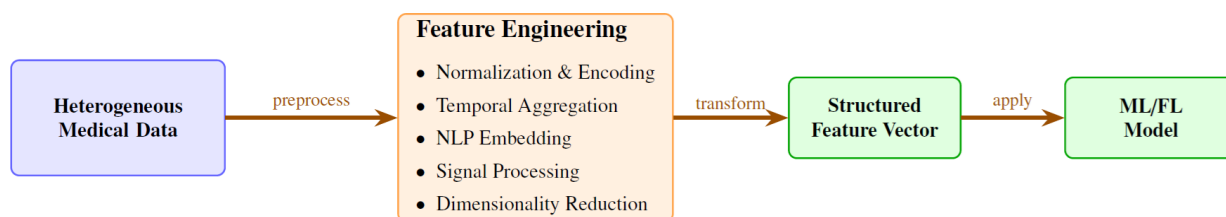
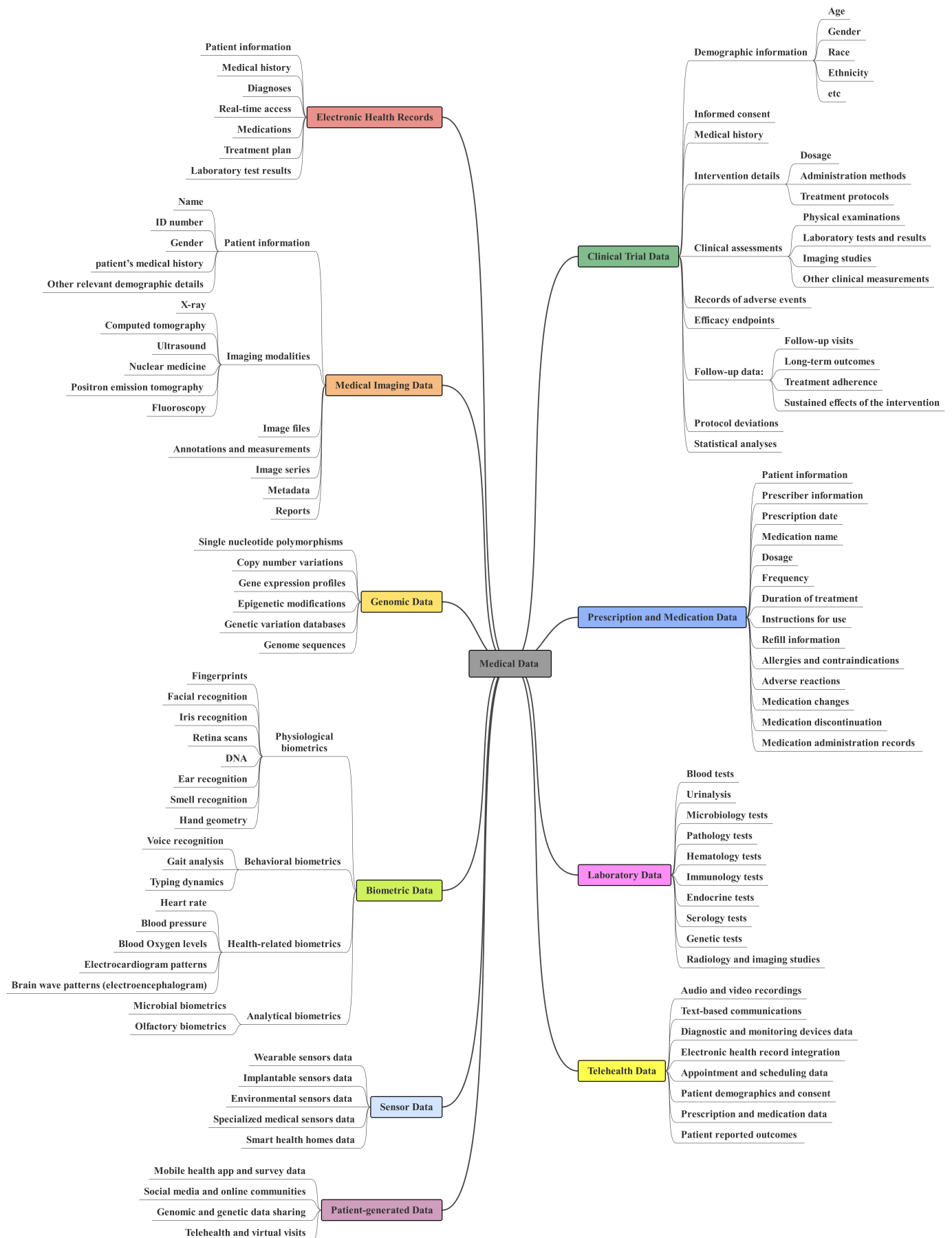


Figure 3. Medical data taxonomy for health care machine learning.



AI and FL in Health Care

Overview

AI is revolutionizing health care, impacting diagnosis, treatment, and patient care. This section explores the evolution of AI in health care, from its historical roots to cutting-edge developments, showcasing its potential across various health care domains. We will further delve into FL as a key technology for the future. FL’s collaborative approach enables privacy-preserving data analysis, making it a powerful tool for health care research and delivery. We will discuss its applications, case studies, current challenges, and future directions.

Potential of AI in Health Care

AI is transforming health care across a wide spectrum, from disease diagnosis to patient care management, making significant contributions in several key areas (Figure 4). The first area is *disease diagnosis and imaging*. AI has revolutionized medical imaging, providing more accurate and faster diagnoses [172]. Deep learning models, trained on large datasets (eg, x-ray images [173], MRI scan images [174], and CT scan images [175]), can identify patterns undetectable to the human eye, aiding in the early detection of diseases like cancer, cardiovascular abnormalities, and neurological disorders. The second area is *drug development and personalized medicine*. AI algorithms streamline drug development by predicting molecular behavior [176] and identifying potential drug candidates [177]. In

personalized medicine, AI analyzes patient data, including genetic information, to tailor treatments, improving efficacy and reducing side effects [123,178]. The third area is *predictive analytics in patient care*. AI’s predictive analytics are crucial to preventive medicine. EHRs are analyzed [179] to predict patient risks for diseases [180], hospital readmission [181], and adverse events, enabling proactive care [180]. The fourth area is *robotics and surgical assistance*. AI-integrated robotics improve surgical precision and outcomes [182]. AI-driven robots assist surgeons in complex procedures, reducing human error and recovery time, and AI supports surgeon training through virtual reality simulations [183]. The fifth area is *patient engagement and telemedicine*. AI-powered chatbots and virtual health assistants provide 24/7 support and health monitoring [184], enhancing patient engagement and adherence. In telemedicine, AI tools assist in remote diagnosis and consultation, making health care more accessible [185]. The sixth area is *health care administration and management*. AI streamlines administrative tasks (scheduling, billing, and claims) [186] and optimizes hospital operations, resource allocation, and patient flow, improving overall efficiency and reducing costs [187]. The seventh area is *global health and epidemic response*. AI is pivotal in tracking and predicting the spread of infectious diseases [188]. During the COVID-19 pandemic, AI models were instrumental in analyzing virus transmission [189], assessing vaccine development [190], and managing health care resources [191]. The key application domains of AI in health care are presented in Figure 5.

Figure 4. Exploring the convergence of artificial intelligence (AI) with health care: trends, applications, and future perspectives. FL: federated learning.

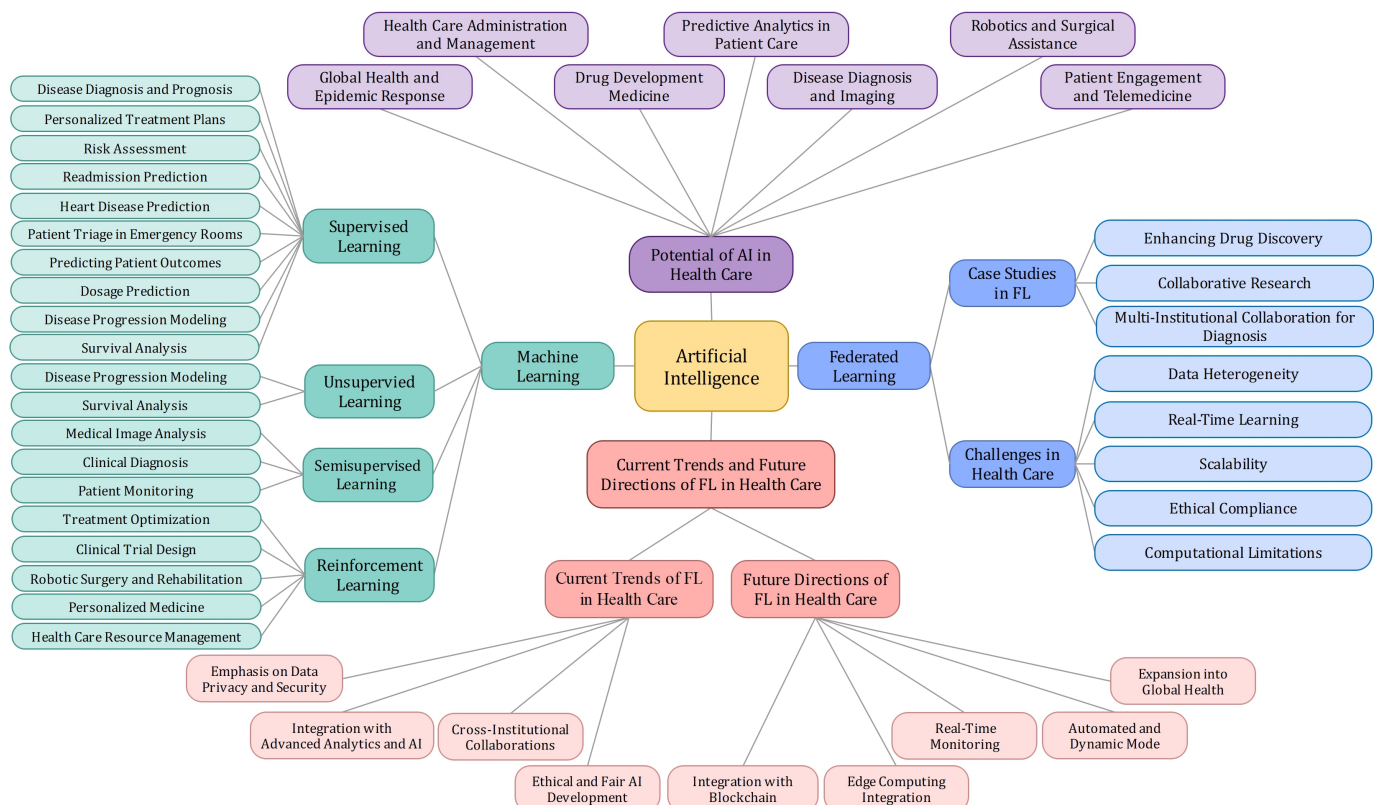
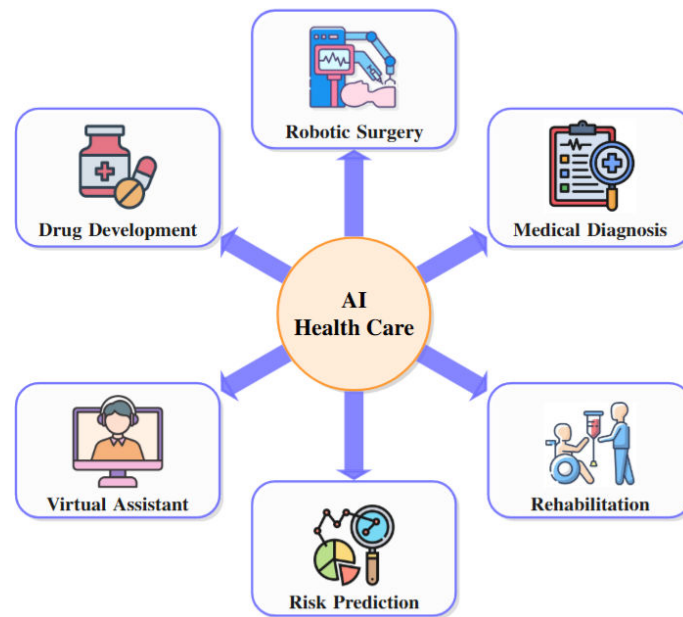


Figure 5. Six key application domains of artificial intelligence (AI) in health care. AI technologies enable advances across drug discovery, surgical precision, diagnostic accuracy, patient rehabilitation, risk assessment, and virtual health assistance.



Fundamentals of ML

ML Background

ML, a pivotal branch of AI, is fundamentally reshaping our approach to problem-solving across various domains, including health care. At its core, ML involves the development and application of algorithms that enable computers to learn from and make decisions or predictions based on data. This capacity for self-improvement and adaptation without explicit programming is what sets ML apart.

The cornerstone of ML is data. Algorithms learn from data patterns, and the quality and quantity of these data significantly influence their performance, as explained in the previous section. ML algorithms are sets of rules or instructions given to computers to help them learn from data. These algorithms can be broadly categorized into supervised learning [192-197], unsupervised learning [198-205], semisupervised learning [206-209], and reinforcement learning (RL) [210-215].

Supervised Learning

Supervised learning, a dominant branch of ML, is crucial in health care, leveraging labeled datasets to train models for making predictions or categorizing data [192]. This approach is powerful where the relationship between the input and output is known and can be modeled [216]. The key characteristics include the following: (1) *labeled data*, training data have known outcomes, guiding the algorithm to learn the relationship between input features and the output; (2) *classification and regression*, the two primary tasks are classification (predicting discrete outcomes, eg, diagnosing a disease) and regression (predicting continuous outcomes, eg, recovery time); and (3) *model training and validation*, the model is trained on one portion of data and validated on a separate, unseen dataset to ensure good generalization.

Supervised learning has a significant impact on health care applications, including the following: (1) *disease diagnosis and prognosis*, ML models are trained on clinical data (symptoms, lab results, and imaging) to identify diseases (eg, models trained on imaging data can detect abnormalities like tumors in radiographic images with high accuracy) [193,194]; (2) *personalized treatment plans*, algorithms analyze patient data to predict individual responses to different treatments, which is effective in fields like oncology [195] where plans are tailored based on tumor genetics; (3) *risk assessment*, models predict the risk of developing conditions (eg, diabetes and heart disease) based on lifestyle, genetics, and other factors [196]; and (4) *readmission prediction*, supervised learning predicts a patient's likelihood of hospital readmission, which is vital for improving patient care and reducing costs [197].

ML offers invaluable tools through its classification and regression tasks. Classification entails categorizing data into predetermined classes, and this is crucial for the following: (1) *disease diagnosis*, models classify patient data into disease categories (eg, using convolutional neural networks to classify dermatological images as benign or malignant skin lesions) [217]; (2) *heart disease prediction*, algorithms analyze patient data (age, blood pressure, and cholesterol level) to classify individuals into risk categories for heart disease, aiding early intervention [218]; and (3) *patient triage in emergency rooms*, models classify patients based on condition severity (analyzing symptoms, vitals, and history) to assist in determining urgency, optimizing patient flow and resource allocation [219].

Regression tasks deal with predicting continuous outcomes in health care, and they are applied to the following: (1) *predicting patient outcomes*, models predict quantitative outcomes like length of hospital stay, surgical recovery time, or disease progression (eg, predicting blood sugar levels in diabetic patients based on lifestyle/medication) [220]; (2)

dosage prediction, regression algorithms predict the optimal drug dosage for individual patients [144], which is particularly important in treatments like chemotherapy to balance efficacy and toxicity [221]; (3) *disease progression modeling*, models forecast the rate of progression for chronic diseases (eg, Alzheimer disease and Parkinson disease) by analyzing patient data over time, aiding treatment planning [222]; and (4) *survival analysis*, regression models are crucial in oncology for predicting patient survival times after diagnosis or treatment, which is vital for planning and management [223].

Unsupervised Learning

Unsupervised learning is a fundamental ML category that analyzes and groups unlabeled data based on similarities and differences, without predefined labels [198]. Two critical techniques are clustering and dimensionality reduction [199-201,203,205,224], and both are vital in genomics and medical imaging.

Clustering groups objects so that those in the same cluster are more similar to each other than to those in other groups. Its health care applications include the following: (1) *genomic data analysis*, clustering categorizes genes with similar expression patterns, aiding in understanding gene functions, identifying disease markers, and revealing biological pathways (eg, it identifies co-expressed gene groups in diseases like cancer, revealing potential therapeutic targets) [199]; (2) *patient stratification*, algorithms segment patients into groups based on similarities in medical records or genetic information [224], and this stratification identifies disease subtypes with distinct clinical outcomes or treatment responses, facilitating personalized medicine; and (3) *medical imaging*, clustering is used for image segmentation (partitioning images into pixel sets) to identify regions of interest, such as tumors in MRI or CT scans, which is crucial for accurate diagnosis and treatment planning [201].

Dimensionality reduction decreases the number of random variables by obtaining a set of principal variables, which is important for dealing with high-dimensional data common in health care as follows: (1) *genomic data analysis*, genomic data are inherently high-dimensional, with techniques like principal component analysis [202] and t-distributed stochastic neighbor embedding [203] reducing their complexity, and this simplification aids in data visualization, identifying genetic markers, and understanding the genetic architecture of diseases; and (2) *medical imaging*, high-resolution images are computationally intensive, and dimensionality reduction techniques reduce the number of features while retaining essential information [204]. This is crucial for efficient storage, processing, and analysis of medical images, facilitating the development of more efficient diagnostic algorithms [205].

Semisupervised Learning

Semisupervised learning is a fundamental ML category uniquely positioned in health care because it improves model performance by leveraging both labeled and unlabeled data [206,208,225]. This approach is cost-effective, utilizing the

abundance of unlabeled data in health care where labeling is often expensive or time-consuming. The key features include the following: (1) *utilizing unlabeled data*, algorithms exploit the vast amounts of unlabeled data in health care databases, which, despite lacking explicit annotations, contain valuable information that complements labeled data and enhances the model's understanding of complex medical phenomena [226]; (2) *combining labeled and unlabeled data*, by incorporating both data types during training, semisupervised algorithms learn more robust representations of the underlying data distribution [227], improving the model's generalization capabilities and leading to more accurate predictions; and (3) *semisupervised techniques*, methods like self-training, co-training, and semisupervised support vector machines iteratively refine predictions using labeled data while leveraging unlabeled data to enhance overall performance [207].

In health care, semisupervised learning applies to diverse areas as follows: (1) *medical image analysis*, algorithms analyze large volumes of unlabeled medical images to identify subtle patterns or anomalies, and combining this unsupervised analysis with labeled data improves the accuracy of tasks such as tumor detection, organ segmentation, and disease classification [209]; (2) *clinical diagnosis*, it assists diagnosis and outcome prediction by leveraging both labeled patient data and unlabeled population health data [208], and this integrated approach enhances diagnostic accuracy and reliability, leading to more informed clinical decisions; and (3) *patient monitoring*, techniques analyze large streams of unlabeled patient data (eg, EHRs and physiological signals) to detect deviations from normal health patterns [225], and incorporating these data into predictive models allows providers to proactively identify and intervene in adverse health events. Overall, semisupervised learning offers a powerful framework to leverage the wealth of unlabeled health care data, advancing ML model performance, medical research, diagnosis, and treatment strategies [228,229].

Reinforcement Learning

RL is an ML type particularly suited for situations where an "agent" must make a sequence of decisions to achieve a goal [230]. Approaches to learning optimal policies include the following: (1) *dynamic programming*, breaks down decision-making into simpler, recursively solved subproblems, which is effective in environments with a perfect, known model (states and transitions); and (2) *Monte Carlo methods*, model-free approaches relying on repeated random sampling to approximate the optimal policy, which is useful for problems with stochastic dynamics and rewards.

In health care, RL offers innovative ways to approach complex, dynamic decision-making problems [210], operating on reward and penalty principles to learn optimal actions through trial and error. The key concepts include the following: (1) *agent and environment*, an "agent" (eg, a health care model) interacts with its "environment" (eg, patient data/scenarios), taking actions and receiving feedback in the form of rewards or penalties based on the outcomes;

(2) *policy*, the strategy the agent uses to determine the next action based on the current environment state (eg, choosing a treatment plan); (3) *reward signal*, guides the agent's actions, with positive rewards encouraging similar decisions and negative rewards signaling adjustment; (4) *value function*, estimates the expected cumulative reward of taking an action in a given state, helping the agent predict long-term outcomes; and (5) *exploration versus exploitation*, balancing trying new actions (exploration) with using known high-reward actions (exploitation), which is analogous to balancing experimental and tried-and-tested treatments.

RL is highly useful in health care applications, including the following: (1) *treatment optimization*, RL adjusts treatment strategies over time based on patient response [211], and for chronic diseases like diabetes, models suggest adaptive insulin dosages, diet, and exercise plans; (2) *clinical trial design*, RL helps determine the most effective trial structures, treatment regimens, and patient selection criteria, enhancing trial efficiency and success rates [231-233]; (3) *robotic surgery and rehabilitation*, used in training robotic systems to adapt to patient-specific conditions and improve based on feedback from surgical outcomes or recovery rates [212]; (4) *personalized medicine*, RL models analyze patient data over time to predict the most effective treatment plans, considering the unique health trajectory and response patterns of each patient [213,214]; and (5) *health care resource management*, algorithms assist in managing resources (hospital bed allocation, staff scheduling, and equipment usage) by learning optimal allocation strategies based on demand and resource availability [215].

Case Studies of ML in Health Care

ML has made significant inroads into health care, transforming patient care, diagnostics, treatment planning, and disease management. Notable real-world examples highlight both successes and challenges as follows: (1) *diagnostic imaging and radiology*, ML (especially deep learning) has revolutionized medical image interpretation (eg, Google Health's ML model outperformed human radiologists in detecting breast cancer in mammograms [234]), and the challenges include integrating these systems into clinical workflows, dealing with diverse data quality, and ensuring consistent performance across different populations and equipment; (2) *drug discovery and development*, ML accelerates drug discovery, reducing cost and time (eg, Atomwise used AI to predict effective molecules, even identifying promising COVID-19 compounds in 2020 [235]), and the primary challenge is the time-consuming and expensive process of validating AI-discovered drugs in clinical trials; (3) *predictive analytics in patient care*, ML models are increasingly used for predictive analytics (eg, the Johns Hopkins team used ML to predict sepsis in hospitalized patients, enabling early intervention [236]), and the challenges include ensuring data privacy, overcoming data silos, and dealing with potential biases in training data; (4) *personalized medicine*, ML aids in tailoring treatments to individual genetic profiles (eg, a team at Earle A Chiles Research Institute used ML to analyze the genetic data of cancer patient for identifying the most effective treatment plans [237]), and the challenges include managing vast

amounts of genetic data, ensuring accurate interpretations, and integrating these insights into routine clinical practice; and (5) *mental health applications*, ML models monitor and diagnose mental health conditions (eg, apps like Ginger.io use ML to analyze user interaction and provide personalized mental health support [238]), and the challenges include addressing privacy concerns, ensuring algorithm sensitivity and specificity across diverse populations, and integrating these tools with traditional mental health services.

FL Details

FL Background

Within the field of ML, data security and privacy are paramount concerns. Traditional ML approaches often require centralized data storage, which can raise privacy issues and limit participation due to data ownership restrictions. FL has emerged as a groundbreaking solution, offering a decentralized paradigm for collaborative ML [239]. In FL, multiple entities, such as health care institutions or research centers, collaborate to train a model without sharing their raw data. Each entity trains a local model on its own data and shares only model updates, such as gradients or parameters, with a central server. This collaborative approach allows for distributed learning while preserving data privacy and security.

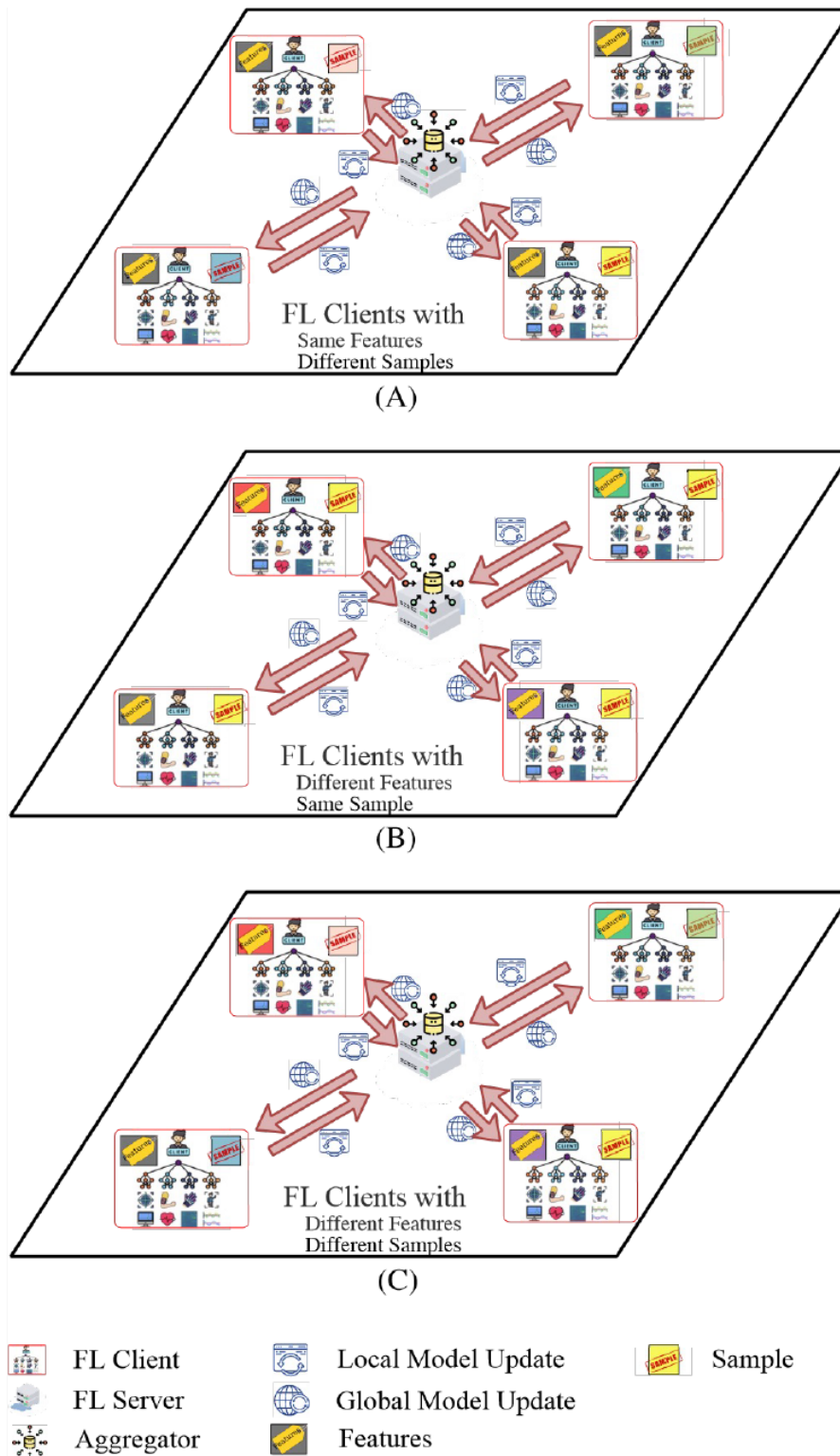
FL Types

FL encompasses three prominent implementations tailored to diverse scenarios and constraints: (1) horizontal FL (HFL); (2) vertical FL (VFL); and (3) federated transfer learning (FTL) (Figure 6). The first implementation *HFL* involves training models across multiple devices or clients that possess similar data distributions (same features) but cannot share raw data due to privacy concerns. Each client trains a local model and shares only model updates (gradients/parameters) with a central server [240]. The server aggregates these updates to refine a global model, which is then redistributed. *HFL* is suitable where data are distributed with similar characteristics, such as mobile phones, IoT edge devices [241], and EEG data [242]. The challenges involve privacy-preserving techniques, communication efficiency, and aggregation strategies [243]. The second implementation *VFL* addresses scenarios where data are distributed across multiple parties with complementary features (different features) that cannot be shared due to privacy/proprietary concerns [244]. Each party holds a subset of features. The goal is collaborative model training without sharing raw data, commonly using secure multiparty computation (SMPC) and HE to enable computation on encrypted data while preserving privacy [245]. *VFL* is applied in health care where different institutions hold complementary patient data (eg, medical records and lab results) that are crucial for accurate models while preserving privacy [246]. The third implementation *FTL* extends traditional transfer learning to federated settings, where knowledge from related tasks or domains is leveraged across multiple decentralized datasets [247]. Unlike traditional transfer learning, *FTL* aggregates knowledge from decentralized clients to refine a base model

(initialized from pretraining or scratch). This accommodates variations in data distributions and characteristics across clients [248]. FTL is beneficial where labeled data are

scarce or unevenly distributed, such as electrocardiogram signal analysis [249], improving performance by leveraging knowledge from related domains.

Figure 6. Types of federated learning (FL): (A) horizontal FL; (B) vertical FL; (C) federated transfer learning.



Case Studies of FL in Health Care

FL holds promise in health care by facilitating the collaborative development of robust ML models across institutions (eg, hospitals and research centers) while safeguarding

patient data privacy [250,251]. This approach trains ML models on local datasets, sharing only model updates (not raw data) to a central server for aggregation, thus mitigating privacy concerns and reducing data transfer costs [252]. FL offers enhanced privacy and utilization of diverse

datasets without centralization. Real-world examples of FL in health care include the following: (1) *multi-institutional collaboration for disease diagnosis*, FL's most significant success involves collaborative projects for disease diagnosis, and an international consortium (including institutions like Massachusetts General Hospital, University of Cambridge, Lahey Hospital, Assuta Medical Centers, Dasa S.A., National Taiwan University, and Seoul National University Hospital) successfully used FL to develop highly accurate models for predicting critical care patient outcomes (eg, mortality and length of stay) by leveraging diverse populations while maintaining data privacy; (2) *enhancing drug discovery and development*, FL has been used in pharmaceutical research to create predictive models for drug response and toxicity, and a notable instance is a project where multiple pharmaceutical companies shared algorithmic models, rather than data, to predict the success of drug compounds, expediting discovery while maintaining confidentiality of proprietary data [253]; and (3) *collaborative research*, FL enables institutions to collaborate on cancer research without sharing sensitive patient data, and a notable example is the collaboration facilitated by Intel and Penn Medicine, utilizing FL to identify brain tumors [254]. These cases demonstrate how FL advances medical research while maintaining data confidentiality.

Challenges of FL in Health Care

FL offers a groundbreaking opportunity to collaboratively develop potent ML models while safeguarding patient data privacy and minimizing transfer costs. However, realizing its full potential in health care requires overcoming significant challenges, including the following: (1) *data heterogeneity and model generalizability*, variability in medical data across institutions (different formats and diverse populations) complicates model convergence and performance, necessitating models that are generalizable to diverse patient populations and data types [255]; (2) *technical and computational limitations*, successful FL implementation requires substantial computational resources and technical expertise that may be unequally distributed among institutions, and balancing these disparities is crucial for success [256]; (3) *regulatory and ethical compliance*, FL must adhere to complex regulations like HIPAA (United States) and GDPR (Europe) governing data privacy and security, and ethical considerations require obtaining patient consent and ensuring equitable distribution of research benefits, necessitating clear data governance and ethical frameworks [257]; and (4) *scalability and real-time learning*, scaling FL models to accommodate real-time learning and large datasets poses technical hurdles, making the efficient management and real-time updating of models challenging [258].

Possible solutions include establishing standardized data formats across entities for consistency, implementing comprehensive data preprocessing pipelines to enhance quality, and designing FL algorithms adept at handling diverse data types and operating effectively across varying computational resources [259].

Future prospects involve integrating FL with emerging technologies like IoT devices and real-time health monitoring systems. This integration could enable the continuous improvement of ML models with real-time data from diverse, distributed sources, leading to more dynamic and responsive health care solutions. Additionally, advancements in edge computing could further enhance FL's efficiency and scalability in health care [260].

Current Trends and Future Directions of FL in Health Care

Overview

The landscape of FL in health care is rapidly evolving, driven by technological advancements and the growing need for collaborative and privacy-preserving data analysis. This section outlines the current trends shaping FL in health care and forecasts its future trajectory.

Current Trends of FL in Health Care

The prevailing trends shaping FL in health care reflect a dynamic evolution toward enhanced analytics, privacy, collaboration, and ethical considerations as follows: (1) *integration with advanced analytics and AI*, FL is being increasingly integrated with sophisticated AI techniques, such as deep learning, to enhance its analytical capabilities [261, 262], and this allows for more complex and accurate models capable of addressing intricate health care challenges like personalized medicine and predictive analytics [250]; (2) *emphasis on data privacy and security*, due to heightened data privacy concerns, FL is gaining traction as a preferred method for collaborative health care research [263], and its inherent design, which allows for model training without sharing raw data, aligns well with stringent data privacy regulations like HIPAA and GDPR; (3) *cross-institutional collaborations*, there is a growing trend of cross-institutional collaborations, as explained previously, which is facilitated by FL, and these collaborations unite hospitals, research centers, and academic institutions, enabling them to pool knowledge and data resources for collective model improvement while maintaining data sovereignty; and (4) *ethical and fair AI development*, there is an increased focus on ethical AI development as FL evolves, ensuring that FL models are fair, unbiased, and representative of all patient demographics, thus addressing concerns around algorithmic bias [19,264,265].

Future Directions of FL in Health Care

FL in health care is poised for significant expansion, driven by emerging technological advancements and evolving health care landscapes. This forthcoming evolution encompasses the following: (1) *expansion into global health initiatives*, FL has the potential to significantly impact global health research, particularly in areas with stringent privacy laws or limited data-sharing capabilities, facilitating the analysis of global health trends and the development of models representative of diverse populations [250]; (2) *automated and dynamic model updating*, the future will likely see more automated and dynamic updating of FL models [266], enabling health care systems to respond quickly to new data or changing health

trends, making the models more adaptive and responsive; (3) *use in remote and real-time monitoring*, with the proliferation of wearable devices and IoT in health care, FL is set to play a significant role in real-time patient monitoring and remote health care, providing personalized insights and treatments based on data from diverse patient populations [267]; (4) *edge computing integration*, integrating FL with edge computing could decentralize computational workload, allowing for faster and more efficient model training and updates, especially in real-time applications [265,268,269]; and (5) *integration with blockchain for enhanced security*, the integration of FL with blockchain technology is a promising development that bolsters data security and adds a layer of transparency and traceability to the FL process, ensuring immutable record-keeping and verifiable model updates in FL networks [13]. In summary, FL in health care is at a dynamic juncture, poised to reshape research and delivery. Its alignment with current needs for privacy, collaboration, and advanced analytics, coupled with its adaptability for future technological trends, positions FL as a key player in the future landscape of health care technology, paving the way for more equitable, secure, and efficient use of health care data globally.

Blockchain

Blockchain Background

Blockchain technology has undergone a remarkable evolution since its inception in 2009 with the creation of Bitcoin by an individual or group using the pseudonym Satoshi Nakamoto [270]. The primary purpose of Bitcoin was to establish a decentralized digital currency, and the innovation that made this possible was blockchain—a distributed ledger that records transactions across a network of computers securely and transparently.

In the following years, the potential applications of blockchain technology expanded beyond cryptocurrency. Vitalik Buterin introduced Ethereum [271] in 2015, introducing the concept of smart contracts—self-executing contracts with the terms of the agreement directly written into code. This development opened up a broader spectrum of decentralized applications (DApps) and laid the foundation for blockchain's role in facilitating not only peer-to-peer (P2P) transactions but also complex programmable interactions.

The years that followed witnessed a surge in blockchain projects and platforms, each aiming to address specific challenges across various industries. The technology gained recognition for its potential to enhance transparency, security, and efficiency. Consortia and collaborations emerged, with enterprises exploring how blockchain could optimize supply chains [272-275], streamline financial transactions, and enhance data integrity.

Blockchain continues to evolve, with ongoing efforts to address scalability issues, energy consumption concerns, and regulatory considerations. From its humble beginnings as the underlying technology for Bitcoin, blockchain has grown into

a versatile tool with the potential to reshape how industries manage and verify data. The technology's journey reflects an ongoing quest for innovative solutions to long-standing challenges in the digital realm.

In this section, we provide a concise overview of fundamental concepts, features, structure, and taxonomy within the realm of blockchain technology.

Blockchain Technology: An Overview

Blockchain technology is a decentralized and distributed ledger system designed to facilitate secure and transparent transactions without the need for a central authority. At its core, blockchain consists of a chain of blocks, each containing a list of transactions. These blocks are linked together in a chronological and immutable manner, forming a continuous chain. One of the key features of blockchain is its decentralization, meaning that the ledger is maintained by a network of nodes rather than a single central entity. This distributed nature enhances security, reduces the risk of fraud, and ensures transparency in the transaction process.

Blockchain technology possesses several distinctive features that contribute to its popularity and versatility across various industries. The features of blockchain technology are as follows: (1) decentralization, (2) immutability, (3) transparency, (4) security, (5) distributed ledger, (6) consensus mechanism, (7) anonymity and privacy, (8) efficiency and speed, (9) interoperability, and (10) ability to support smart contracts. First, regarding decentralization, blockchain operates on a P2P network, eliminating the need for a central authority or intermediary, and this enhances security, reduces the risk of a single point of failure, and promotes trust among mutually untrusted participants [276]. Second, immutability is the capability of a blockchain ledger to remain unchanged. Once a block is added to the blockchain, it becomes virtually impossible to alter or delete the information within it. Immutability ensures the integrity of the transaction history and builds trust in the accuracy of recorded data. Third, regarding transparency, the entire transaction history is visible to all participants in the network, and this fosters trust and accountability as participants can independently verify transactions and the state of the blockchain. Fourth, regarding security, blockchain uses cryptographic techniques to secure transactions and control access to the network. Consensus mechanisms, such as proof of work (PoW) and proof of stake (PoS), enhance security by preventing unauthorized changes to the blockchain [277-279]. Fifth, the ledger is distributed among the nodes over the network, and each node in the network holds a copy of the blockchain. This distribution ensures redundancy, resilience, and a shared source of trust among the participants. Sixth, consensus is a mechanism that gives the network the ability to agree upon the validity of transactions (and blocks) and the order in which they can be added to the blockchain. Seventh, regarding anonymity and privacy, while all transactions in the blockchain network are transparent, participants remain pseudonymous due to the use of public/private key pairs. Eighth, regarding efficiency and speed, blockchain reduces the need for intermediaries and manual processes,

leading to faster and more efficient transactions. In some cases, however, the speed of transactions may depend on the specific consensus mechanism used. For instance, PoW blockchains, like Bitcoin, tend to be slower (ie, with less throughput) compared to traditional payment systems like Visa and Mastercard. The primary reasons for this include the inefficiency of the underlying consensus mechanisms and the way transactions are processed [280]. Ninth, blockchain interoperability refers to the capacity of various blockchain networks to interact seamlessly, facilitating the exchange of messages, data, and tokens among them [281-285]. Standards and protocols are evolving to enable such communication and data exchange between disparate blockchain platforms. The Inter-Blockchain Communication (IBC) protocol [286] is designed to facilitate this interoperability by providing a standardized way for independent blockchains to transfer and communicate with each other. Tenth, regarding the ability to support smart contracts, smart contracts are self-executing contracts with the terms directly written into code. These contracts automate and enforce predefined rules and agreements, reducing the need for intermediaries and streamlining processes [287,288].

Consensus Mechanism in Blockchain

Consensus in the context of blockchain refers to the mechanism by which a distributed network of nodes agrees on the state of the system or the validity of transactions [289-291]. Since blockchain operates in a decentralized and trustless environment, consensus is crucial to ensure that all participants have a consistent view of the blockchain's history and current state. The consensus mechanism is responsible for preventing double-spending (where the same digital asset is spent more than once) and maintaining the integrity of the blockchain. Different blockchain networks use various consensus algorithms, each with its own set of rules and processes. The most prominent and currently existing consensus protocols are as follows: PoW; PoS; Byzantine fault tolerance (BFT); directed acyclic graph (DAG); and hybrid consensus, including PoS and PoW hybrid, proof of authority (PoA) and PoW hybrid, delegated PoS (DPoS) and PoA hybrid, PoW and BFT hybrid, and hybrid voting system.

PoW Protocol

This is the original consensus algorithm used by Bitcoin [270] and many more cryptocurrencies. In PoW, participants (miners) solve complex mathematical puzzles to validate transactions and create new blocks. The first miner to solve the puzzle gets the right to add a new block to the blockchain. PoW is resource-intensive and requires a significant amount of computational power [292]. Blockchains that rely on PoW are more prone to forks. A fork in blockchain technology refers to a split in the blockchain's transaction history, resulting in two or more separate paths. This can occur for various reasons, such as changes in protocol rules, disagreements among participants, or software upgrades [293].

PoS Protocol

In PoS [294], validators (ie, block proposer participants) are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. This eliminates the need for energy-intensive mining and aims to provide a more energy-efficient alternative to PoW. Examples include Ethereum's [295] transition to Ethereum 2.0, Cardano [296], and Algorand [297]. DPoS is an improvement over traditional PoS in terms of scalability and efficiency [298].

BFT Protocols

BFT consensus algorithms are a class of protocols designed to achieve consensus in distributed systems, even in the presence of faulty or malicious nodes. In a BFT-based consensus algorithm, a network of nodes collaborates to agree on the state of the system or the validity of transactions. The term "Byzantine fault" originates from the Byzantine generals' problem [299], a theoretical scenario where a group of generals must come to a unanimous agreement on a coordinated action, despite the possibility of some generals being traitors and sending conflicting messages. Practical BFT (pBFT) is the most prominent variant of BFT-based consensus protocols [300]. This algorithm is designed to tolerate up to one-third of the total number of nodes being faulty or malicious. This means that as long as no more than one-third of the nodes in the network exhibit Byzantine behavior (ie, they may fail arbitrarily or behave maliciously), pBFT can still reach consensus and continue to operate correctly. Some variants of BFT (eg, Hotstuff [301], pBFT, and improved BFT) are supported by Hyperledger Fabric [302].

DAG Protocols

DAG consensus protocols are a class of distributed consensus algorithms that use a data structure called a directed acyclic graph to achieve agreement on the order of transactions or events in a decentralized network. Unlike traditional blockchain-based consensus protocols where transactions are organized into linear blocks, DAG-based protocols organize transactions in a more flexible graph structure [303]. One of the most well-known implementations of DAG consensus is the tangle [304], which is used in the IOTA cryptocurrency network [305]. In the tangle, each transaction directly references and approves 2 previous transactions, forming a directed acyclic graph structure. The most prominent blockchains that run on proof of capacity include Signum, Chia, and SpaceMint.

Hybrid Consensus Protocols

Overview

Hybrid consensus models in blockchain combine elements of multiple traditional consensus mechanisms to leverage their respective strengths and mitigate their weaknesses. These models aim to achieve a balance among decentralization, security, scalability, and energy efficiency [306]. Some hybrid consensus models in blockchain are described below.

PoS and PoW Hybrid

Some blockchain networks combine PoS and PoW mechanisms to achieve consensus (eg, TwinsCoin [307]). For example, a PoW component may be used for initial block creation, while PoS is utilized for subsequent block validation or as a way to elect validators. This hybrid approach aims to maintain security through PoW while improving scalability and energy efficiency with PoS.

PoA and PoW Hybrid

In this hybrid model, a network may utilize PoW for initial block creation and PoA for block validation. PoW ensures the initial distribution of tokens and secures the network against Sybil attacks, while PoA provides fast finality and scalability by relying on known and trusted validators.

DPoS and PoA Hybrid

DPoS allows token holders to vote for a limited number of delegates who are responsible for block validation. In a hybrid approach, DPoS can be combined with PoA, where the initial set of validators is determined through PoA, and then, token holders can vote for additional delegates using DPoS. This hybrid model aims to achieve both decentralization and scalability.

PoW and BFT Hybrid

This hybrid model combines the energy-intensive PoW with a BFT-based consensus algorithm such as pBFT or Tendermint [308]. PoW is used for block creation, while BFT consensus ensures finality and fault tolerance. This approach aims to achieve both security and efficiency in blockchain networks [309].

Hybrid Voting Systems

Some blockchain networks combine different voting mechanisms, such as direct voting by token holders and voting by elected delegates [310]. This hybrid voting system aims to balance the influence of token holders with the expertise and accountability of elected representatives.

Blockchain Data Structure

In blockchain technology, the data structure plays a pivotal role in ensuring the integrity, security, and immutability of the distributed ledger [278,311]. At its core, a blockchain is composed of a series of blocks, each containing a bundle of transactions. These blocks are cryptographically linked together sequentially, forming a continuous chain. The data structure of a block typically includes several key components: a header, a list of transactions, and a cryptographic hash. The header contains metadata, such as the block's unique identifier (block hash), a timestamp, and a reference to the previous block's hash, thus establishing the chronological order of blocks. The transaction list records the details of all transactions included in the block, such as sender and receiver addresses, transaction amounts, and cryptographic signatures for verification. Additionally, each block is assigned a cryptographic hash, which is computed based

on its contents using a hashing algorithm like SHA-256. This hash serves as a unique identifier for the block and is crucial for maintaining the integrity of the blockchain. Any alteration to the data within a block would result in a change in its hash, thereby breaking the chain's continuity and signaling tampering. The inherent immutability and tamper-resistance of the data structure in blockchain ensure that once recorded, transactions cannot be altered or deleted without consensus from the network participants, establishing a reliable and transparent system for recording and verifying transactions [312].

Blockchain Network and Architecture

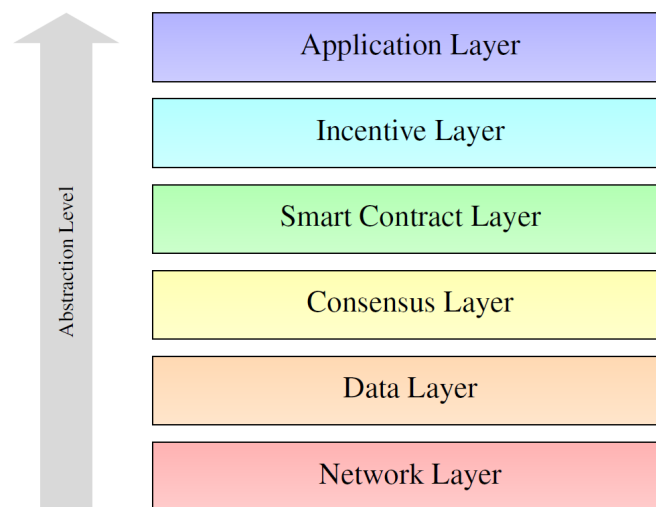
The network architecture in blockchain is a distributed and decentralized system that enables the secure and transparent exchange of data and value across a network of interconnected nodes. At its core, a blockchain operates as a P2P network where each participant, or node, maintains a copy of the entire blockchain ledger. This distributed architecture ensures that there is no single point of failure, as the data are replicated and synchronized across multiple nodes. Nodes communicate with each other through a consensus mechanism. Depending on the consensus algorithm used, nodes may take on different roles, such as miners in the PoW system or validators in the PoS system. Transactions are broadcast to the network and validated by consensus, typically requiring confirmation from a majority of nodes before being added to the blockchain. This network architecture provides several benefits, including resilience against censorship and tampering, increased transparency and accountability, and enhanced security through cryptographic techniques.

Additionally, the decentralized nature of blockchain networks promotes trust among participants by eliminating the need for intermediaries and central authorities, thereby fostering a more inclusive and democratic ecosystem for conducting transactions and exchanging value [313].

Blockchain technology typically consists of 6 common layers, each serving a specific purpose in the network's function and security (Figure 7). The six layers are as follows: (1) *network layer*, the foundation facilitating communication between nodes using protocols like TCP/IP, HTTP, and P2P protocols, responsible for transmitting data (transactions and blocks) across the network; (2) *data layer*, stores the actual blockchain data, including blocks, transactions, and smart contracts, utilizing structures and storage mechanisms optimized for secure and efficient retrieval; (3) *consensus layer*, ensures all nodes agree on the validity and order of transactions added to the blockchain using various mechanisms, such as PoW, PoS, DPoS, and pBFT; (4) *smart contract layer*, enables the creation and execution of programmable, self-executing contracts with terms written directly into code, powering various DApps; (5) *incentive layer*, provides mechanisms (typically block rewards and transaction fees, eg, Bitcoin's block rewards and Ethereum's gas fees) to incentivize participants (miners or validators) to contribute resources and maintain the network's security and integrity; and (6) *application layer*, encompasses the user-facing applications and interfaces (eg, DApps, wallets,

smart contracts, and other software) that interact with the blockchain protocol.

Figure 7. Six-layer blockchain architecture illustrating increasing abstraction from the network layer to the application layer.



IBC Protocol

Interoperability is one of the most important features of next-generation blockchain networks and refers to the ability of different blockchain platforms to communicate, share data, and transact with each other seamlessly. It enables interoperability between disparate blockchain networks, allowing them to interact and exchange information or assets without the need for intermediaries or centralized exchanges. Interoperability is essential for realizing the full potential of blockchain technology by facilitating cross-chain transactions, asset transfers, and data sharing between different blockchain ecosystems [286].

The IBC protocol is a set of standards and protocols designed to enable communication and interoperability between independent blockchain networks. IBC facilitates the secure and trustless transfer of assets and data across different blockchains, allowing them to interact and transact with each other directly. The protocol defines a standardized messaging format and a set of rules for validating and verifying transactions between participating blockchains. By implementing the IBC protocol, blockchain networks can establish interconnectivity, enabling cross-chain transactions, decentralized exchanges, and interoperable DApps [283,314,315].

IBC is a pillar of the Internet of Blockchains [311,316], a vision where blockchain networks are interconnected like the global internet, creating a decentralized and open ecosystem where data, assets, and services flow freely between different blockchains. Examples of interoperability solutions include the following: (1) *Cosmos*, a decentralized network utilizing the IBC protocol to enable communication and interoperability between its various blockchain platforms, with the Cosmos Hub serving as the primary connection point [317]; (2) *Polkadot*, a multichain blockchain platform that enables interoperability between different parachains (parallel

blockchains) within its network via its relay chain, allowing them to share data and assets seamlessly [318]; and (3) *Wanchain*, a cross-chain blockchain platform focused on interoperability, enabling the secure and decentralized exchange of assets between different blockchain networks, including Bitcoin and Ethereum [319].

Blockchain Taxonomy

Overview

At a high level, blockchain networks are classified into 3 main categories: private, public, and consortium blockchains. These are briefly explained in the following subsections.

Private Blockchain

A private blockchain is a permissioned blockchain network where access and participation are restricted to authorized entities only. These entities typically have known identities and are granted permission to join the network by a central authority or administrator. Private blockchains are often used by enterprises and organizations to build internal blockchain solutions for specific use cases such as supply chain management, document verification, and intercompany transactions. They offer enhanced privacy, control, and scalability compared to public blockchains [320,321]. For instance, Hyperledger Fabric is a private blockchain framework developed by the Linux Foundation's Hyperledger project [302,322,323]. It is designed for enterprise use cases and enables organizations to create permissioned blockchain networks with customizable features and governance models.

Public Blockchain

A public blockchain is a permissionless blockchain network that is open to anyone to join, participate, and transact without requiring permission or identification. Public blockchains are decentralized networks where transactions are transparent,

immutable, and verifiable by anyone. They offer high levels of transparency, censorship resistance, and security but may sacrifice scalability and privacy due to their open nature [324-327]. Public blockchains are often used for cryptocurrencies, DApps, and tokenized assets. For instance, Bitcoin operates as a decentralized P2P network for sending and receiving the Bitcoin cryptocurrency.

Consortium Blockchain

A consortium blockchain is a semidecentralized blockchain network governed by a consortium or group of organizations rather than a single centralized entity. Consortium blockchains are permissioned networks where the consensus process and governance are shared among a predefined set of participants. Consortium blockchains are commonly used in industries or sectors where multiple organizations collaborate on shared processes or infrastructure while still maintaining some level of control and privacy [328-331]. They offer a balance between the decentralization of public blockchains and the control of private blockchains. For instance, R3 Corda is a consortium blockchain platform developed by the enterprise blockchain consortium R3. Corda is designed for use cases that require privacy, scalability, and interoperability in multiple organizations from sectors such as finance, health care, and supply chain.

Integration of FL With Blockchain

Overview

Integrating blockchain technology with FL has emerged as a novel approach to address inherent data privacy, security, and trust challenges within distributed ML systems [21,23,332,333]. FL, characterized by training ML models across decentralized devices without centrally aggregating raw data, offers significant advantages in preserving user privacy and data confidentiality. In other words, in federated ML, the exchange occurs at the parameter level instead of transmitting raw data. This approach mitigates the risk associated with centralized computing architectures, which are susceptible to targeted attacks and potential denial of service due to their single-point-of-failure vulnerability. A detailed discussion on FL is presented in the FL Details section, including its different types (HFL, VFL, and FTL), applications (particularly in health care), and potential future directions (integration with advanced analytics and cross-institutional collaborations), highlighting FL's pivotal role in reshaping health care technology.

However, concerns persist regarding the integrity of FL systems, particularly regarding data tampering or manipulation by malicious or compromised nodes. Blockchain, renowned for its immutable and transparent ledger capabilities, presents a compelling solution to these challenges. By leveraging blockchain's decentralized consensus mechanisms and cryptographic primitives, FL systems can ensure data integrity, traceability, and transparency throughout the ML model training process [334-336]. Moreover, blockchain's smart contract functionality enables the establishment of

auditable and self-executing agreements among participants, further enhancing the trustworthiness of FL collaborations [23]. This integration not only addresses privacy and security concerns but also fosters a more collaborative and inclusive environment for distributed ML research and applications. As such, the motivation behind the integration of blockchain and FL lies in the pursuit of enhancing data privacy, security, and trust in decentralized ML ecosystems, ultimately advancing the adoption and efficacy of FL methodologies in various domains such as health care [13,336,337].

Blockchain technology holds immense potential to significantly enhance the security, transparency, and trustworthiness of FL systems by addressing key challenges like verifying local model updates, aggregating the global model, and incentivizing participants. The integration of blockchain into FL is explored as follows: (1) verifying local model updates, (2) global model aggregation, and (3) incentivizing participants. First, regarding verifying local model updates, blockchain offers an immutable and tamper-proof record for local model updates from participants. These updates are recorded as transactions, ensuring their validity and preventing unauthorized modifications. Furthermore, smart contracts can be used to define specific rules, and they function as verification mechanisms, executing algorithms to validate the integrity and accuracy of updates [338]. Second, regarding global model aggregation, blockchain empowers FL with decentralized consensus mechanisms (eg, PoW and PoS) that allow participants to collectively agree on the process of aggregating the global model. The entire aggregation process is transparently recorded on the blockchain, allowing participants to verify the fairness and accuracy of the final model [339]. Third, regarding incentivizing participants, a key strength of blockchain is its ability to create tokenized incentives (tokens or cryptocurrencies) to reward participants who contribute data or computational resources [340]. Smart contracts automate the distribution of these incentives based on predefined criteria (eg, quality of contribution and computational resources provided) [341]. Crucially, the entire distribution process is transparently recorded on the blockchain, ensuring accountability and fairness [342].

By leveraging the unique strengths of blockchain technology, FL systems can achieve a new level of security, transparency, and trust, ultimately fostering a more collaborative and efficient environment for AI development.

Integration Architecture

Several research efforts have identified distinct architectures for integrating blockchain and FL. This paper proposes a framework similar to that in a previous report [343], with slight variations in terminology. Based on the level of interaction between blockchain and FL entities, we categorize these architectures as fully coupled, semicoupled, and loosely coupled.

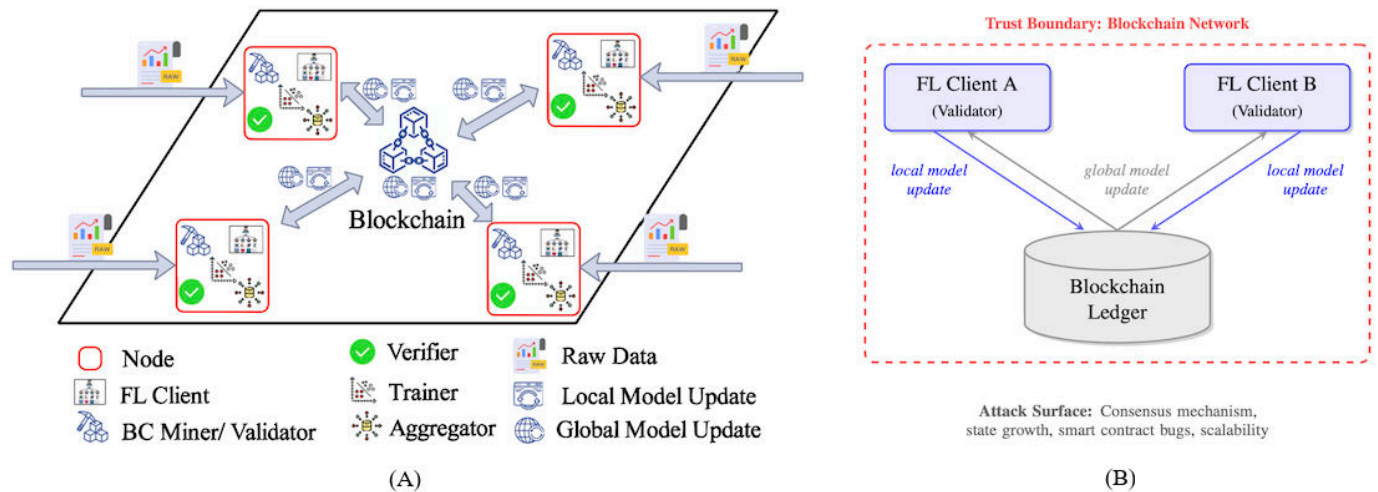
Fully-Coupled Architecture

In the fully-coupled architecture, blockchain nodes (ie, miners or validators) perform dual roles as FL clients. Within this

architecture, FL clients engage in computing local model updates as well as validating these updates as blockchain nodes. Notably, blockchain nodes not only partake in training local models but also participate as the global model aggregator. The aggregator, which may be a selected node, a designated leader, or a collection of nodes based on the predefined protocol, is responsible for gathering local model updates. Every node in this model has the opportunity to

function as a blockchain validator, a local model trainer, and a global aggregator concurrently. Consequently, both local model updates and global model updates are contained within the blockchain. Importantly, the absence of a necessity to transmit the global model to a central server mitigates the risk of a single point of failure within this architecture. A schematic of this architecture is depicted in Figure 8.

Figure 8. Fully-coupled blockchain-based federated learning (FL) architecture: (A) detailed architecture; (B) schematic diagram. All local updates are committed on-chain via a smart contract that performs aggregation. Clients act as validators within a unified blockchain trust domain.

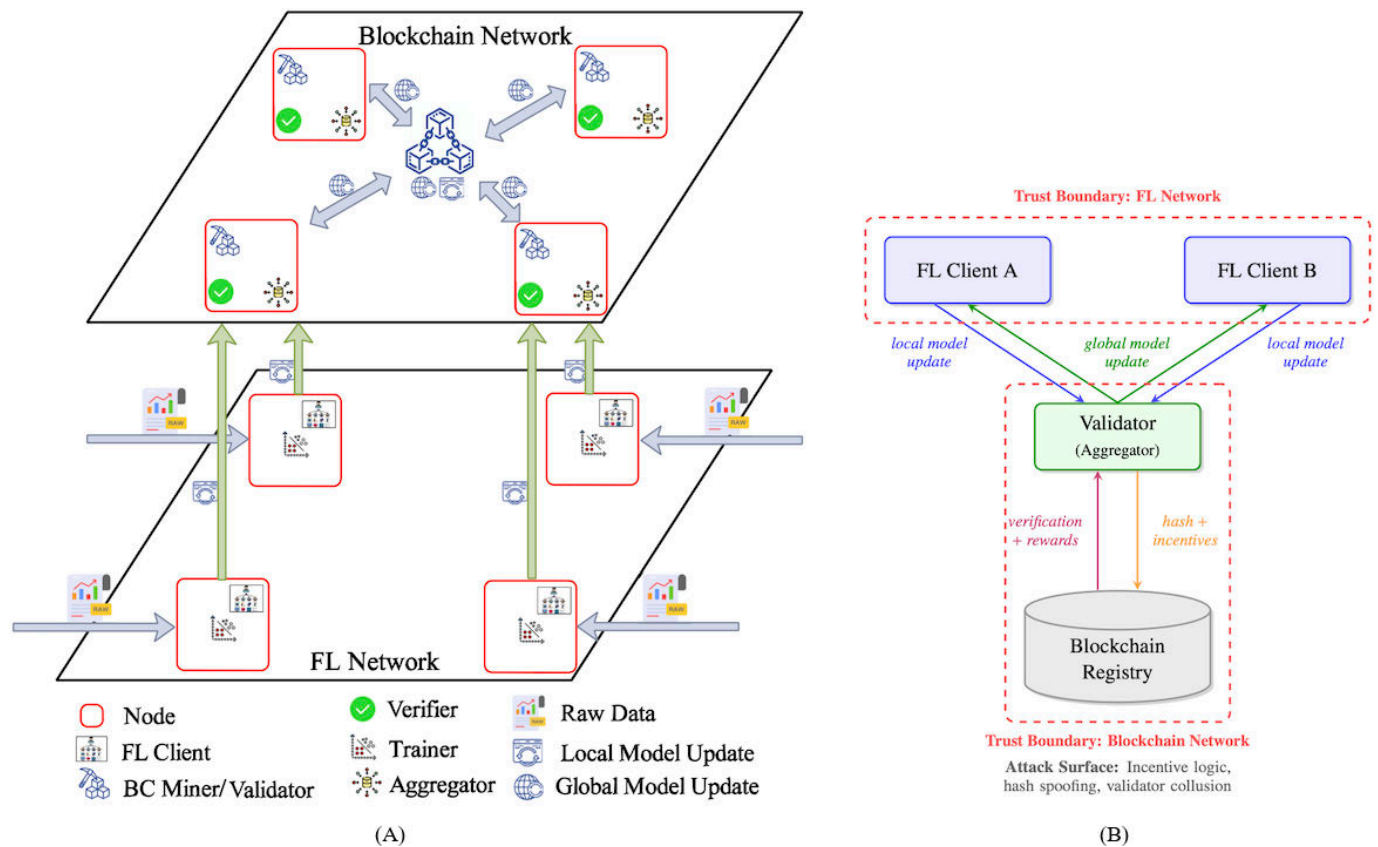


Semicoupled Architecture

In the semicoupled architecture, blockchain and FL clients inhabit separate networks, although FL clients retain the capability to interact with the blockchain and manipulate the distributed ledger. FL clients gather data from diverse sources, train local models, and subsequently upload local model updates to the blockchain. Blockchain nodes (ie, miners or validators) are tasked to validate the uploaded local

model updates that will be used for training the global model. Upon the preparation of the global model, blockchain nodes will store it within the blockchain. Participant rewards are allocated based on a predefined incentive mechanism. This architecture also circumvents the potential for a single point of failure. A schematic of this architecture is depicted in Figure 9.

Figure 9. Semicoupled blockchain-based federated learning (FL) architecture: (A) detailed architecture; (B) schematic diagram. Validators perform aggregation off-chain with an on-chain registry and incentives.

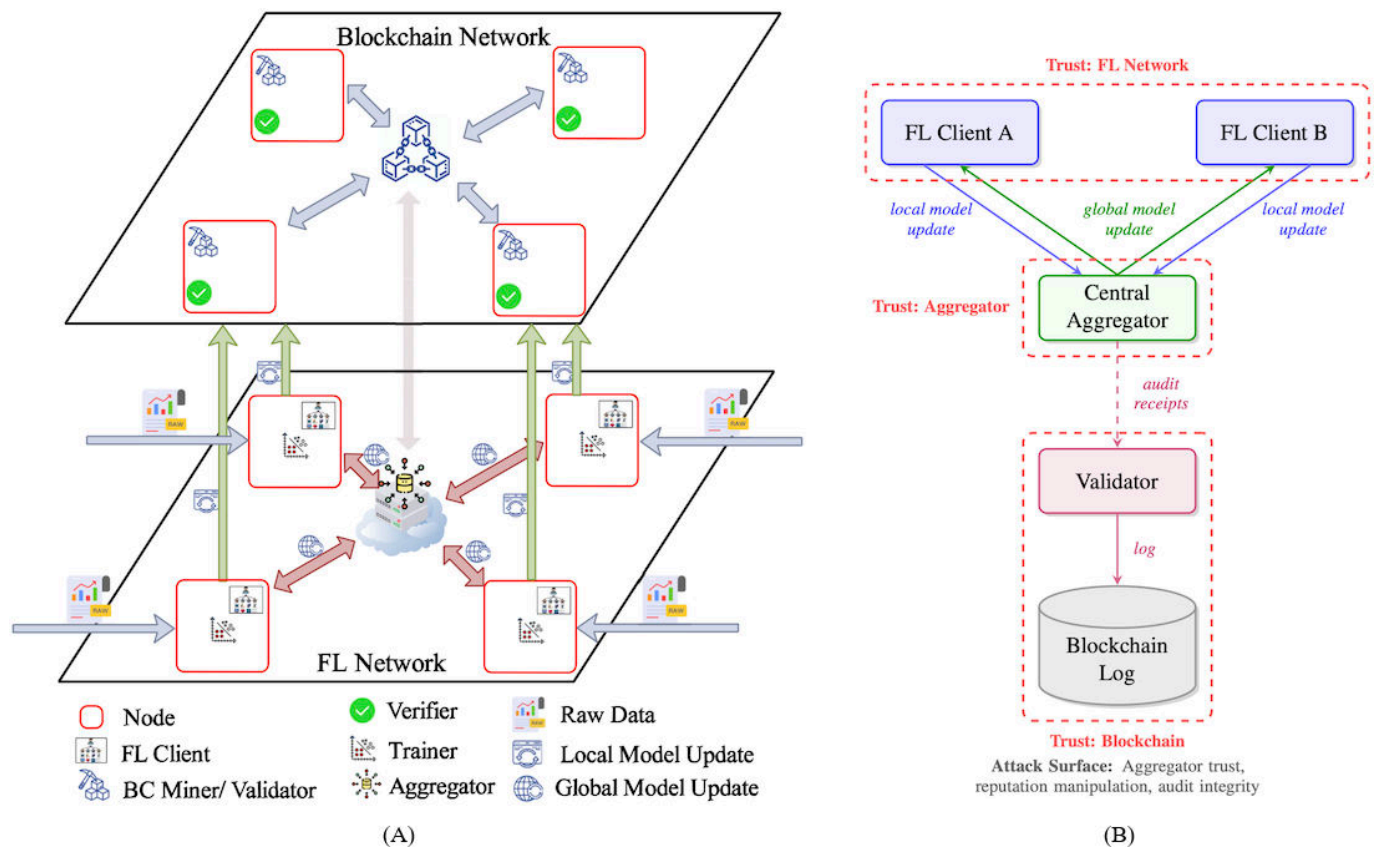


Loosely-Coupled Architecture

In the loosely-coupled architecture, blockchain nodes and FL clients are in 2 distinct networks. This architecture introduces reputation as a criterion for measuring the reliability of the clients. In this architecture, the primary function of the blockchain is to furnish a coordination mechanism for clients, manage their reputation, handle authentication, manage validation of local model updates, and manage incentives (ie, contributions are managed to ascertain reputation and

incentivize participation). While the blockchain validates local model updates, it refrains from storing them. In contrast, it stores data related to the reputation of the participants. The responsibility of the FL clients is to train local models and upload updates to the blockchain for validation. After validation, these updates are sent to an aggregator, which can be a distinct server or a cloud space. A schematic of this architecture is depicted in [Figure 10](#).

Figure 10. Loosely-coupled blockchain-based federated learning (FL) architecture: (A) detailed architecture; (B) schematic diagram. Central aggregator with blockchain used only for audit logs.



Cross-Architecture Synthesis and Quantitative Cost Analysis

The 3 BCFL integration patterns examined above represent distinct points on a design spectrum trading decentralization for performance and operational simplicity. The fully-coupled design maximizes audibility by executing all operations on-chain, but incurs significant latency (bounded by the blockchain finality time t_f) and ledger state growth, limiting scalability to small consortia (≤ 50 clients). The semicoupled

design achieves a pragmatic balance by performing model aggregation off-chain while recording verifiable provenance and incentive information on-chain, supporting medium-scale health care deployments (≤ 100 clients). The loosely-coupled design minimizes blockchain interaction, using it primarily for coordination and audit, offering high throughput for large IoMT or regional networks (≥ 200 clients). Practitioners can map deployment size, regulatory constraints, and trust requirements to these design points to select an optimal integration pattern, as summarized in Table 2.

Table 2. Comparative characteristics and quantitative cost trends across blockchain-based federated learning integration architectures.^a

Characteristic	Fully-coupled architecture	Semicoupled architecture	Loosely-coupled architecture
Trust model	Fully decentralized (all clients act as validators)	Partially decentralized (off-chain aggregation, on-chain proofs)	Federated trust (central aggregator with optional audit)
Latency per round	High ($\sim t_f^b$; consensus limited)	Medium (off-chain aggregation, on-chain logging)	Low (minimal blockchain interaction)
Throughput/scale	≤ 50 clients	≤ 100 clients	≥ 200 clients
Compute overhead Δ_{BC}	12%-15% (cryptographic + consensus tasks)	5%-8% (hashing + verification)	2%-4% (logging + coordination)
Network cost pattern	Full model updates transmitted on-chain	Partial metadata and incentive records	Receipts and coordination only
On-chain storage/round	$C^c q^d / W^e$ (hundreds of MBs)	10-100 kB	$C \times 0.3$ to 1 kB
Auditability	Very high (complete lifecycle recorded)	High (key model lineage and incentives)	Moderate (hash receipts only)
Best use	High-security, small-scale consortia	Balanced health care networks	Large-scale IoMT ^f or regional systems

^aTypical health care configuration: clients per round (C) = 50, model size (W) = 80 MB (FP32), compression ratio (q) = 0.1, global rounds (R) = 200, finality time (t_f) = 1 to 10 s, client churn rate (λ) \approx 0.05.

^b t_f : finality time.

^c C : clients per round.

^d q : compression ratio.

^e|W|: model size.

^fIoMT: Internet of Medical Things.

The quantitative cost model formalizes these tradeoffs. The per-client computational load combines local training and blockchain overhead as follows: $FLOPs_{client} \approx E n f (1 + \Delta_{BC})$, where E represents local training epochs per round, n represents samples in the local dataset, f represents floating-point operations per sample, and Δ_{BC} represents blockchain overhead from cryptographic signing, consensus participation, and data serialization. Empirical studies report Δ_{BC} values of approximately 2%-4% for the loosely-coupled design, 5%-8% for the semicoupled design, and 12%-15% for the fully-coupled design [339,344].

Network usage grows linearly with communication rounds as follows: $Bytes_{client} \approx 2q |W| R(1 + \lambda)$, where $|W|$ represents model parameter size, q represents the compression ratio ($0 < q \leq 1$), R represents total rounds, and λ represents the client churn rate. The factor of 2 accounts for upload and download traffic. Storage requirements differ sharply for the loosely-coupled design ($C \times 0.3$ to 1 kB/round), semicoupled design (10 to 100 kB/round), and fully-coupled design ($Cq|W|$ /round). For typical health care configurations, fully-coupled deployments require approximately 400 MB on-chain per round and approximately 3.2 GB total transfer per client, which are considered impractical for most BFT blockchains [302,345], whereas semicoupled and loosely-coupled designs reduce bandwidth by 40%-50% with a submegabyte on-chain state. Round latency is lower-bounded by finality time t_f , which increases with validator set size N_v due to $O(N_v^2)$ message complexity of the BFT consensus [345,346]. Consequently, the fully-coupled design suits small, high-security networks, while the loosely-coupled design offers practical scalability for large federations.

Assumptions and Scope

All values are order-of-magnitude estimates derived under synchronous federated averaging [347] and BFT blockchain configurations (eg, Hyperledger Fabric [302] and Tendermint [348]). While real-world performance may vary with model architecture, bandwidth, or consensus protocol, the relative scaling behavior and architectural tradeoffs among computation, communication, and on-chain costs remain consistent across implementations, including asynchronous or adaptive variants.

Security and Privacy Considerations

Overview

Integrating FL and blockchain addresses security and privacy challenges inherent in collaborative health care learning. While FL enhances privacy by training models on local datasets, it introduces vulnerabilities like model poisoning, gradient leakage (potential for patient reidentification), and coordination failures [349].

Blockchain mitigates these risks via its immutable, decentralized framework, strengthening FL through the

following: (1) *immutable audit trails*, every model update, contribution, and access event is cryptographically recorded and timestamped on the blockchain, creating a verifiable and transparent history for forensic investigation [350]; (2) *decentralized trust and consensus*, blockchain eliminates reliance on a central authority, distributing trust across nodes to enhance resilience against single points of failure; and (3) *cryptographic security*, mechanisms ensure data integrity, authenticity, and nonrepudiation for all transactions and model updates, reinforcing the overall trustworthiness.

To further enhance privacy and compliance in BCFL systems, the following advanced cryptographic and security techniques are used: (1) ZKPs, (2) HE, (3) SMPC, (4) trusted execution environments (TEEs), and (5) DP. First, ZKPs enable participants to prove compliance (eg, data quality and consent) without revealing underlying sensitive patient data, allowing verifiable protocol adherence while safeguarding privacy [351,352]. However, ZKPs face substantial computational challenges, limiting practical applicability in real-time clinical systems [353,354]. Second, HE permits computation on encrypted data, enabling secure aggregation of model updates [352,355]. Although improved, HE introduces computational overhead (eg, 3.7 times to 8.2 times in health datasets) that presents scalability concerns and requires specialized hardware in resource-constrained settings [356]. Third, SMPC enables joint computation of aggregate functions (eg, model averaging) over private inputs without revealing individual contributions, offering strong privacy during aggregation [357,358]. SMPC protocols introduce significant computational and communication overhead through intensive cryptographic operations, posing a challenge in bandwidth-constrained health care networks [359,360]. Fourth, regarding TEEs, hardware-based secure enclaves provide isolated computation for sensitive operations (eg, aggregation) with cryptographic attestation [361,362]. However, TEEs suffer from memory limitations necessitating layer-wise training (performance overhead) and remain vulnerable to side-channel attacks (eg, cache timing and speculative execution) that can compromise confidentiality [363,364]. Fifth, DP introduces controlled noise to model updates or gradients for quantifiable privacy guarantees [365]. DP introduces critical privacy-utility tradeoffs (eg, 1%-3% accuracy reduction in COVID-19 models), and the required privacy budget calibration is challenging, especially in non-independent and identically distributed health care data settings where noise and heterogeneity can slow model convergence [366,367].

Threat Model for BCFL in Health Care

We define a comprehensive threat model for BCFL systems in health care, identifying adversaries, capabilities, attack objectives, and mitigation strategies. This model provides a formal foundation for understanding security guarantees and tradeoffs, enabling practitioners to select appropriate defenses for specific deployment scenarios.

Adversaries and Capabilities

The BCFL ecosystem faces four adversary classes as follows: (1) *malicious clients*, these are compromised health care institutions or IoMT devices executing data poisoning, model poisoning [6,368], free-riding, or inference attacks with full access to local training processes; (2) *malicious aggregators*, these are present in loosely-coupled or semicoupled architectures, and they may infer private data from updates, bias global models through selective exclusion, or manipulate aggregation; (3) *Byzantine validators*, they comprise colluding blockchain nodes approving invalid updates, double-spending incentive tokens, or disrupting consensus; and (4) *external adversaries*, they include passive eavesdroppers intercepting communications, performing traffic analysis, or executing membership inference attacks.

Attack Objectives

Adversaries pursue distinct objectives through various attacks as follows: (1) *integrity attacks*, corrupt model reliability through model poisoning [6,368,369], backdoor insertion [370,371], and Sybil attacks, potentially causing misdiagnosis; (2) *privacy attacks*, extract patient data via

gradient inversion [372-374], membership inference [375, 376], and model inversion, violating HIPAA and GDPR guidelines; (3) *availability attacks*, disrupt services through denial-of-service on FL coordination, blockchain consensus, or participants, impacting clinical decision support; and (4) *fairness attacks*, introduce demographic biases or exclude underrepresented populations [377], exacerbating health care disparities.

Threat Mitigation

Table 3 maps threats to mitigation techniques with quantified performance implications from the Empirical Validation and Performance Evaluation section. These mitigations provide complementary protection layers deployable based on application requirements. Byzantine-robust aggregation [368,378] maintains integrity with up to 30% compromised participants but incurs 3%-5% accuracy degradation. HE provides semantic security with 3.7 to 8.2 times computational overhead [379]. DP [380] offers formal (ϵ, δ)-privacy guarantees with 1%-3% accuracy reduction, as observed in COVID-19 models.

Table 3. Threat mitigation mapping for blockchain-based federated learning in health care.

Threat	Mitigation	Security guarantee	Cost
Model poisoning	Byzantine-robust aggregation (Krum, FLTrust) [368]; Reputation systems	Resilient to $\leq 30\%$ malicious clients	3%-5% accuracy drop
Gradient leakage	HE ^a [352]; SMPC ^b [379]	Semantic security for updates	HE: 3.7 to 8.2 times overhead
Membership inference	DP ^c [380,381]; Gradient masking	(ϵ, δ)-privacy	1%-3% accuracy loss
Free-riding	Proof of federated work [382,383]; Tokenized incentives	Verifiable contribution	On-chain verification overhead
Model inversion	ZKPs ^d [351]; TEEs ^e	Verifiable computation	ZKPs: 8-15 s proof time
Consensus attacks	BFT ^f protocols (PBFT ^g , IBFT ^h) [300,345]	Tolerates less than one-third Byzantine nodes	$O(N^2)$ ⁱ message complexity

^aHE: homomorphic encryption.

^bSMPC: secure multiparty computation.

^cDP: differential privacy.

^dZKPs: zero-knowledge proofs.

^eTEEs: trusted execution environments.

^fBFT: Byzantine fault tolerance.

^gPBFT: practical Byzantine fault tolerance.

^hIBFT: improved Byzantine fault tolerance.

ⁱ $O(N^2)$: quadratic time complexity.

Architectural Security Tradeoffs

The 3 BCFL architectures provide distinct security-performance tradeoffs. Fully-coupled architectures maximize security through on-chain execution but incur approximately t_f latency per round and 12%-15% overhead, and they are suitable for high-security consortia with stringent audit requirements. Semicoupled architectures balance security and performance through selective on-chain logging, maintaining strong auditability with 5%-8% overhead and supporting up to 100 participants. Loosely-coupled architectures optimize scalability with minimal blockchain interaction, and they are suitable for large-scale IoMT deployments but require stronger trust in the central aggregator.

Empirical validation shows that these layered mitigations maintain accuracy within 2%-3% of nonprivate baselines. Combining DP ($\epsilon < 0.1$) with encrypted updates sustains utility, with an approximately 2.8 times compute overhead, while Byzantine robust aggregation maintains less than 5% degradation with up to 30% compromised clients. Mitigation selection should be guided by regulatory compliance (HIPAA/GDPR), data sensitivity, and clinical impact on patient outcomes.

Practical Deployment Challenges

The integration of privacy-enhancing technologies into health care involves technical intricacies regarding compatibility, efficiency, and communication overhead [12]. FL requires uniform infrastructure and capabilities across all

sites, and unreliable infrastructure can disrupt training [384]. Cross-institutional coordination is amplified by complex data governance, regulatory requirements (eg, HIPAA and GDPR), and heterogeneous resource constraints [344]. Methodological flaws (eg, privacy issues, generalization, and communication costs) have rendered most recent FL health care studies inappropriate for clinical use [385].

Integration architecture significantly impacts tradeoffs as follows: (1) the fully-coupled architecture provides maximum auditability by logging all FL operations on-chain (highest security) but faces scalability challenges due to blockchain throughput limitations and consensus inefficiency, particularly with traditional PoW or basic PoS [344,386]; (2) the semicoupled architecture balances security and performance by selectively recording critical events (eg, model updates) on-chain while keeping routine operations off-chain; and (3) the loosely-coupled architecture offers the greatest scalability by using blockchain primarily for coordination and incentives, relying on off-chain security for the learning process, but it requires additional trust assumptions. Emerging architectures utilize sidechains to address scalability by enabling parallel processing and faster verification [386]. Addressing implementation challenges requires continued advancement in specialized hardware acceleration (eg, DARPA’s FHE-focused DPRIVE project [387]),

adaptive privacy mechanisms, and standardized protocols for cross-institutional deployments.

Operational Resilience and Failure Modes

Beyond cryptographic security, BCFL operational resilience requires predefined failure protocols with consortium-approved, measurable triggers. We define the following policy parameters: τ_{quorum} (minimum client quorum), Θ_{round} (round deadline), τ_{byz} (maximum tolerated Byzantine clients for robust aggregation [388]), δ_{AUROC} (maximum allowed area under the receiver operating characteristic curve drop), δ_{ECE} (maximum allowed expected calibration error increase), $\tau_{\text{PSI}}^{\text{major}}$ (population stability index bound for major drift), τ_{txfail} (transaction failure rate bound), and ϵ_{post} (postupgrade error rate threshold). All thresholds are established during pilot deployments, documented in consortium standard operating procedures (SOPs), and calibrated to each clinical task’s criticality and site capabilities. Table 4 summarizes these operational playbooks, specifying for each failure mode its trigger condition, automated response procedures, and monitoring signals, and the associated on-chain audit events. These playbooks link directly to the verifiability and auditability layer discussed in the Auditability and Verifiability in BCFL section, ensuring that every remediation event is immutably logged and cryptographically attestable on-chain.

Table 4. Operational failure protocols for blockchain-based federated learning in health care (thresholds set via governance).

Failure mode	Trigger condition	Response playbook	Monitoring signals	Audit events
Client dropout	Quorum $< \tau_{\text{quorum}}^a$ after Θ_{round}^b ; Byzantine clients $> \tau_{\text{byz}}^c$	Proceed with partial aggregation using Byzantine-robust methods [388]; checkpoint current state; suspend chronic offenders; re-enroll upon verification	Participation rate, round latency, missing sites, straggler ratio	Round degraded, site suspended, site reenrolled
Model drift	AUROC ^d drop $> \delta_{\text{AUROC}}^e$; ECE ^f increase $> \delta_{\text{ECE}}^g$; PSI ^h $> \tau_{\text{PSI}}^{\text{major}i}$	Pause promotion; perform shadow evaluation; rollback if unresolved; initiate root cause analysis	AUROC by cohort, ECE by cohort, PSI, drift alerts	Drift alert, model freeze, model promote, model rollback
Contract upgrade	Security vulnerability, policy change, or tx ^j failure rate $> \tau_{\text{txfail}}^k$	Execute time locked multisig proxy upgrade; perform staged rollout; autorevert if postupgrade errors $> \epsilon_{\text{post}}^l$	tx failure rate, version mismatch, event gaps	Upgrade proposed, upgrade executed, upgrade reverted
Key compromise	Unexpected signer behavior, attestation failure, or CRL ^m entry detected	Revoke key; rotate via threshold MPC ⁿ [389]; reattest using HSM ^o /TEE ^p ; reaggregate any tainted data	Signature verify fail rate, unexpected signer count, anomalous payouts	Key revoked, key rotated, site re-enrolled

^a τ_{quorum} : minimum client quorum.

^b Θ_{round} : round deadline.

^c τ_{byz} : maximum tolerated Byzantine clients for robust aggregation.

^dAUROC: area under the receiver operating characteristic curve.

^e δ_{AUROC} : maximum allowed AUROC drop.

^fECE: expected calibration error.

^g δ_{ECE} : maximum allowed ECE increase.

^hPSI: population stability index.

ⁱ $\tau_{\text{PSI}}^{\text{major}}$: PSI bound for major drift.

^jtx: transaction.

^k τ_{txfail} : transaction failure rate bound.

^l ϵ_{post} : postupgrade error rate threshold.

^mCRL: certificate revocation list.

ⁿMPC: multiparty computation.

^oHSM: hardware security module.

^pTEE: trusted execution environment.

Case Study: Multi-Institutional Brain-Tumor Segmentation

To concretely illustrate these operational protocols, we consider BCFL deployment for glioblastoma segmentation across 3 academic medical centers (hospitals A, B, and C) utilizing the federated tumor segmentation benchmark [390]. Hospital A serves as the semicoupled aggregator in this consortium. The workflow encompasses the following: (1) *data types and preparation*, where each institution contributes multimodal DICOM MRI scans (T1, T1Gd, T2, and FLAIR sequences) accompanied by expert-annotated segmentation masks for enhancing, necrotic, and edema tumor subregions; (2) *consent and governance*, managed through smart contracts encoding tiered patient permissions that allow model training, permit secondary research (opt-in), and prohibit commercial use; (3) *training execution*, where each hospital trains a local 3D U-Net model on its data, computing gradient hashes $h(\nabla W_i)$ submitted to the blockchain via the ModelUpdate smart contract after each federated round; and (4) *operational resilience*, demonstrated when hospital B experiences a network outage mid-round—the system automatically proceeds using the quorum threshold $\tau_{\text{quorum}} = 0.67$ (the quorum threshold $\tau_{\text{quorum}} = 0.67$ ensures BFT consistent with standard BFT safety guarantees $[n \geq 3f + 1]$, allowing global aggregation to proceed only when at least two-thirds of clients contribute authenticated updates), and after 3 consecutive missed rounds, hospital B is suspended until manual infrastructure verification. This end-to-end scenario demonstrates how BCFL protocols maintain continuity in collaborative clinical research despite real-world operational challenges.

Regulatory-Compliant Integration

Overview

The integration of blockchain with FL in health care environments requires strict adherence to comprehensive

regulatory frameworks governing patient data protection, medical device validation, and cross-jurisdictional data exchange. This section analyzes architectural approaches for achieving regulatory compliance while preserving the security and privacy benefits of BCFL.

Regulatory Framework Overview

Health care data processing operates under multiple regulatory frameworks with stringent requirements for data handling, storage, and sharing. In the United States, HIPAA [391] establishes comprehensive privacy and security standards for protected health information (PHI), mandating administrative, physical, and technical safeguards [15]. Similarly, the GDPR [392] in the European Union requires explicit consent for data processing, adherence to data minimization principles, and provision of data portability and erasure rights. These regulatory requirements create significant challenges for conventional centralized ML approaches, often requiring detailed audit trails, comprehensive data lineage tracking, and the ability to selectively remove individual patient contributions from trained models [393].

The proliferation of AI and ML in medical applications has introduced additional regulatory considerations. The FDA framework for AI/ML-based medical devices emphasizes transparent model development, continuous performance monitoring, and the ability to track model behavior across diverse patient populations [394]. These requirements align well with BCFL capabilities, where immutable audit trails and decentralized validation mechanisms provide the transparency and accountability necessary for regulatory compliance in distributed settings [394].

Table 5 maps these key regulatory obligations to concrete FL and blockchain design mechanisms, highlighting how BCFL architectures can be engineered to support compliance across HIPAA, GDPR, and FDA requirements.

Table 5. Mapping of HIPAA^a, GDPR^b, and FDA^c requirements to FL^d and blockchain design mechanisms.

Guideline and key requirement	FL plus blockchain design mechanisms
HIPAA	
Privacy: PHI ^e confidentiality; Security: electronic PHI, integrity/availability; Minimum necessary use	FL data locality, encrypted model updates, blockchain stores only hashed metadata (not PHI); Permissioned blockchain with BFT ^f consensus, tamper-evident logs, redundant FL storage; Local feature selection, DP ^g and gradient clipping, blockchain smart contracts enforce data policies
Audit controls	Immutable blockchain ledger for access/update logs, fine-grained access control lists, cryptographic signatures
Transmission security	TLS ^h for FL channels, authenticated blockchain overlays, health care public key infrastructure integration
GDPR	
Lawfulness, fairness, transparency; Purpose limitation; Data accuracy; Right to erasure	Blockchain consent smart contracts, transparent logging, explainable FL models; Task-specific FL models, local data filtering, blockchain policies restrict model reuse; Cross-institutional FL validation, blockchain model lineage, rollback capability; Off-chain personal data, blockchain pseudonymous references, key revocation and model forgetting
Privacy by design	FL with DP/secure aggregation, minimal on-chain data, role-based blockchain permissions
Data protection impact assessment	Blockchain logs as impact assessment evidence, threat modeling, anomaly detection for poisoning/leakage
FDA	

Guideline and key requirement	FL plus blockchain design mechanisms
Software as a medical device lifecycle control; Good machine learning practice and validation	Blockchain-anchored model versioning, immutable training/deployment records; Federated evaluation across sites, blockchain-backed data/model provenance
Postmarket monitoring	Continuous FL updates, blockchain logs for drift/adverse events, auto-rollback triggers
Change management	Blockchain registry for approved versions, on-chain governance for model rollout
Cybersecurity integrity	Signed FL/blockchain nodes, remote attestation, blockchain-based software bill of materials/model bill of materials tracking

^aHIPAA: Health Insurance Portability and Accountability Act.

^bGDPR: General Data Protection Regulation.

^cFDA: Food and Drug Administration.

^dFL: federated learning.

^ePHI: protected health information.

^fBFT: Byzantine fault tolerance.

^gDP: differential privacy.

^hTLS: transport layer security.

Compliance Challenges in FL

Traditional FL implementations face several compliance challenges in health care environments [395]. Data governance becomes complex when training spans multiple institutions with different privacy policies and jurisdictional requirements. Cross-border data sharing restrictions, exemplified by national data localization laws, can limit the scope of federated collaborations [396]. The distributed nature of FL can complicate compliance auditing, as conventional centralized monitoring approaches are inadequate for tracking model updates and validating data usage across multiple participating nodes. Model explainability requirements present another challenge, given increasing regulatory demands for transparent decision-making processes in clinical AI systems [397]. The aggregated nature of federated model updates can obscure individual data source contributions, hindering the provision of detailed explanations required for regulatory compliance and clinical validation.

Blockchain-Enhanced Compliance Architecture

Blockchain technology provides fundamental mechanisms that directly address regulatory compliance requirements in federated health care systems. The immutable distributed ledger creates comprehensive audit trails that record all model updates, participant contributions, and data access events, satisfying requirements for detailed recordkeeping and accountability. Smart contracts can automate compliance verification by embedding regulatory requirements directly into the blockchain protocol, ensuring that data sharing and model training activities automatically conform to predefined privacy and security standards.

The 3 integration architectures offer varying degrees of compliance capabilities. First, for the fully-coupled architecture, all FL operations are recorded on the blockchain ledger, providing maximum transparency and auditability. Each model update is cryptographically signed and time-stamped, creating an immutable record of the entire training process. This architecture suits environments requiring the highest levels of regulatory oversight but may face scalability constraints with high-frequency model updates. Second, the semicoupled architecture is a hybrid approach

that selectively records critical compliance events on the blockchain while maintaining routine operations off-chain. Compliance-relevant activities, such as participant authentication, consent management, and model validation, are tracked on-chain, while frequent model updates occur off-chain with periodic on-chain checkpoints. This balance provides robust compliance capabilities while addressing scalability concerns. Third, for the loosely-coupled architecture, the blockchain primarily serves as a coordination and reputation management layer, with detailed compliance tracking implemented through conventional audit mechanisms. This approach offers maximum flexibility for integration with existing health care IT infrastructure but requires careful design to ensure adequate regulatory compliance.

Auditability and Verifiability in BCFL

Beyond confidentiality and integrity guarantees, BCFL must also provide transparent mechanisms for independent verification and traceability of all learning activities. To ensure transparent operations, verifiability and auditability in BCFL are defined as complementary properties that enable independent validation of all training activities without compromising privacy. Verifiability denotes the ability of any authorized entity to cryptographically confirm the authenticity and integrity of model updates, aggregation results, and participating institutions through signed digital evidence recorded on-chain. Auditability extends this notion by enabling authorized auditors to reconstruct and verify the entire lifecycle of the learning process (including the provenance of training rounds, participant consent scope, and compliance checks) using immutable ledger entries and corresponding off-chain records.

In the proposed framework, each local model update (ΔW_i) is hashed (eg, SHA-256) and digitally signed by the participant before being submitted to the blockchain. The on-chain record contains the following: (1) the participant's pseudonymous identifier, (2) the signed update hash, (3) the round number and timestamp, (4) a consent-proof token (linking to consent metadata stored off-chain), and (5) the result of automated policy-compliance checks executed via smart contracts. Full model parameters, gradients, raw medical data, and detailed computational logs remain off-chain within secure institutional storage to preserve privacy and

reduce blockchain overhead. This hybrid design allows auditors to verify consistency between on-chain commitments and off-chain artifacts, providing cryptographically verifiable evidence of model provenance, policy adherence, and regulatory compliance while maintaining confidentiality of protected health information.

Case Study: Regulatory Verification

Building upon brain-tumor segmentation deployment, a health care regulator conducts comprehensive compliance verification through systematic analysis of on-chain evidence across the following four critical dimensions: (1) *consent verification*, achieved by querying the ConsentRegistry smart contract to cryptographically validate that all training data possess active consent tokens with appropriate scope limitations and no revocation events during the model training period; (2) *model provenance audit*, tracing the complete lineage of the global segmentation model through immutable, timestamped update records that capture each hospital's contribution sequence and aggregation proofs, thereby creating an auditable chain of custody from raw gradients to the final model; (3) *policy compliance validation*, verifying through smart contract execution logs that every model update underwent automated HIPAA security rule validation and Institutional Review Board (IRB) requirement checks prior to integration into the global model; and (4) *data governance assurance*, confirming through ZKP attestation that all patient data processing remained within institutional boundaries, with only cryptographic commitments—never raw medical images or sensitive patient information—traversing the network. This comprehensive verification process, fully reconstructible from blockchain evidence, demonstrates how the semicoupled BCFL architecture (Figure 9) enables rigorous regulatory oversight. The on-chain audit trail provides concrete verification artifacts, as follows:

Block #18345: $\text{hospital}_A \rightarrow h(\nabla W_A) + \text{timestamp} + \text{consent proof} + \text{HIPAA check}$; Block #18346: $\text{hospital}_C \rightarrow h(\nabla W_C) + \text{timestamp} + \text{consent proof} + \text{HIPAA check}$; Block #18347: $\text{aggregator} \rightarrow h(W_{\text{global}}) + \text{aggregation proof} + \text{ZKP attestation}$

This immutable record preserves patient privacy through cryptographic guarantees while maintaining institutional autonomy through verifiable local computation.

Cross-Border Compliance Considerations

International health care collaborations must navigate different regulatory requirements across jurisdictions [398]. BCFL architectures can incorporate jurisdiction-specific compliance rules through modular smart contract designs. Participants from different regulatory environments can implement their local compliance requirements while engaging in collaborative model training. The blockchain ledger can maintain separate compliance tracks for different jurisdictions [399], ensuring each participant's regulatory obligations are met while enabling global collaboration. Data localization requirements are addressed through FL's inherent data locality principle, where sensitive patient data remain within its originating jurisdiction. The blockchain

component facilitates cross-border collaboration by managing model updates and coordination without requiring direct data sharing, satisfying both privacy regulations and data sovereignty requirements.

Implementation Guidelines for Regulatory Compliance

Successful deployment of regulatory-compliant BCFL requires careful attention to several implementation considerations. Organizations must establish clear data governance frameworks that define roles, responsibilities, and accountability measures for all participating entities [400]. Consent management systems must be integrated into the blockchain architecture to ensure patient permissions are tracked and honored throughout the FL process [12]. The technical infrastructure must support both the scalability demands of FL and the audit trail requirements of regulatory compliance [401]. This includes implementing robust key management systems for cryptographic operations, establishing secure communication channels between participating nodes, and designing backup and recovery procedures that maintain compliance during system failures. Regular compliance auditing must be embedded in the system design, with automated monitoring capabilities to detect potential regulatory violations and alert administrators to compliance issues. The blockchain's immutable audit trail provides the foundation for these monitoring systems, enabling continuous compliance verification and rapid response to potential violations.

Ethical and Patient-Centric Considerations

Beyond regulatory and technical safeguards, ethical considerations are essential for responsible BCFL deployment in health care. The decentralized nature of FL and blockchain complicates the acquisition and management of patient consent across autonomous institutions with diverse governance frameworks [402,403]. Traditional consent models, designed for single-institution data use, are inadequate when patient data contribute to shared models with different stakeholders and objectives [402]. To address this, consent management should leverage verifiable cryptographic mechanisms, such as consent tokens, ZKPs, and smart contract-based registries, to enable patients to grant, track, and revoke permissions without disclosing sensitive data [12, 404]. These mechanisms uphold autonomy and transparency while aligning with evolving interpretations of HIPAA and GDPR.

Blockchain immutability also conflicts with the GDPR's "right to be forgotten" (Article 17) [405,406]. To reconcile this, BCFL designs should store personally identifiable data off-chain while recording only hash-based consent attestations and model metadata [407,408]. This preserves auditability and enables consent withdrawal without breaching immutability.

Fairness is equally critical, as institutions with greater computational capacity or larger datasets may dominate model updates, biasing outcomes against underrepresented

groups [409,410]. Mitigation requires fair aggregation [403], representative datasets [411], and fairness-aware or distributionally robust optimization ensuring consistent performance across demographics [412,413].

Ethical governance mechanisms, including IRBs [414, 415] and data ethics councils [416,417], should oversee consent processes, fairness evaluations, and the protection of vulnerable populations [414,418]. Clear accountability across AI developers, health care providers, and blockchain participants is vital [419]. Finally, explainable AI approaches [420-422] must ensure that model decisions are interpretable by clinicians and understandable to patients, reinforcing trust and autonomy. Ethical BCFL thus requires a shift from a compliance-driven design to a patient-centric design, where transparency, fairness, and accountability become foundational principles for building trust and ensuring sustainable adoption of collaborative health care AI systems [402,423].

Ethics and Patient Voice

Ethical deployment of BCFL in health care requires patient-centric design, translating consent, autonomy, and transparency into actionable system features. Consent should evolve from binary opt-in to granular, preference-based models, allowing patients to specify which data types (eg, EHRs, genomic data, and imaging data) and purposes are permitted through layered interfaces [424,425]. A revocation mechanism records consent withdrawal as an on-chain event, preventing further participation. While revocation cannot retroactively remove previously aggregated updates, federated unlearning protocols mitigate historical influence by efficiently retraining global models without revoked participants [426,427]. Meaningful transparency extends beyond cryptographic verifiability to interpretable communication, and systems should notify contributors when models trained on their data are deployed and provide accessible indicators of model performance, bias, and fairness. When BCFL outcomes inform clinical decisions, explainable AI (XAI) techniques (eg, Shapley Additive Explanations [SHAP] and confidence decomposition) support instance-level explanations that bridge distributed model complexity with clinician and patient understanding [422,428,429].

Embedding granular consent, verifiable revocation, and interpretable transparency within the BCFL architecture ensures that distributed health care AI respects patient autonomy; aligns with regulatory obligations under HIPAA, GDPR, and the FDA’s AI/ML-based SaMD action plan

[430]; and fosters sustained public trust in collaborative health systems [431].

Future Regulatory Developments

The regulatory landscape for AI in health care continues to evolve, with new guidelines and requirements emerging regularly. BCFL architectures must be designed with flexibility to accommodate changing regulatory requirements without requiring a complete system redesign. The modularity of smart contract-based compliance frameworks provides this adaptability, enabling organizations to update their compliance mechanisms as regulatory requirements evolve. Emerging regulatory trends, such as algorithmic accountability requirements and mandatory AI explainability, are well-suited to blockchain-based approaches that provide transparent audit trails and verifiable model development processes. As health care organizations increasingly adopt AI and ML technologies, the compliance advantages of BCFL will become increasingly important for regulatory acceptance and clinical adoption.

Empirical Validation and Performance Evaluation

Overview

This section grounds our BCFL integration in evidence from clinical deployments, consortia-scale studies, and controlled benchmarks. We synthesize outcomes along four axes: (1) accuracy versus centralized baselines; (2) scalability and latency/throughput under permissioned consensus; (3) robustness and privacy under realistic threat models; and (4) compliance, provenance, and operational constraints. Where possible, we report representative ranges from cited studies rather than single-point claims.

Large-Scale Clinical and Multi-Institutional Evidence

Table 6 summarizes emblematic deployments. Across drug discovery (MELLODDY [253]), neuro-oncology (federated tumor segmentation [390]), pandemic diagnostics [432], and IoMT monitoring [251,433], BCFL consistently delivers accuracy within approximately 2%-3% of centralized training while providing auditability and coordination via permissioned chains or distributed ledgers.

Table 6. Representative blockchain-based federated learning deployments in health care.

Setting/cohort	Scale	Task	Blockchain role	Accuracy	Latency/overhead	Source
MELLODDY (10 pharma companies)	>2.6 billion data points, 21 million compounds	Drug prediction	Distributed ledger for auditability, consensus, traceability	Median ~2% RIPTOP ^a gain	Comparable to centralized	[253]
FeTS ^b (71 sites)	71 international sites	Brain tumor segmentation	Coordination and registry	Within 2%-3% of centralized	Real-world federation	[434,435]

Setting/cohort	Scale	Task	Blockchain role	Accuracy	Latency/overhead	Source
COVID-19 consortium	Multinational	CT ^c scan diagnosis	Aggregation logging, verification	94.2% versus 95.1% centralized	~3.2 s/round	[433]
IoMT ^d monitoring	50 patients	Anomaly detection	Consent, notarization	92.7%	<5 s for alerts	[436,437]
EHR ^e management	Multi-institutional	Clinical analytics	Model validation, audit trails	95.2%	<150 ms blockchain latency (10,000 transactions)	[344]

^aRIPtoP: relative improvement of proximity to perfection.

^bFeTS is primarily a federated learning platform; blockchain integration is demonstrated in other health care applications listed here.

^cCT: computed tomography.

^dIoMT: Internet of Medical Things.

^eEHR: electronic health record.

Performance and Scalability Benchmarks Architectural Tradeoffs

Controlled experiments report stable training under 50-200 participants with permissioned consensus, and recent empirical studies demonstrate that blockchain-enabled FL can reduce communication overhead by 40%-60% through communication-aware aggregation schemes [339, 344]. Specifically, there was a 43% communication overhead reduction and a 37% lower computational cost while maintaining 95.2% model accuracy [344]. Sharded or committee-based designs sustain 80-120 TPS at the consortium scale while keeping the consensus overhead under 5% for ≤ 50 nodes, and at 100 nodes, PBFT-style protocols exhibit 12%-15% overhead [438,439].

Security, Privacy, and Robustness

Against gradient inversion and membership inference, combining DP (eg, $\epsilon < 0.1$) with encrypted or masked updates sustains utility within 3%-5% of nonprivate baselines at an approximately 2.8 times compute overhead, while Byzantine-robust aggregation maintains <5% degradation under up to 30% compromised clients [19,352]. Recent work has demonstrated that blockchain-enabled frameworks maintain robustness against multiple adversarial attack vectors with accuracy levels above 93% [344]. For verifiable compliance, ZKPs amortize to proof generation of 8-15 s and verification of 2-4 s per minute-scale update [440].

Compliance, Provenance, and Operational Considerations

Empirical audits indicate technical adherence to approximately 93% of HIPAA/GDPR provisions, with 70%-80% manual audit effort reduction when provenance is automated via smart contracts [395]. For FDA transparency obligations on AI/ML devices, immutable lineage reduces evidence cycles from an initial 6-9 months to 2-3 months in reported pipelines [397]. Operational deployment of blockchain-enabled FL systems faces several infrastructure challenges, including maintaining high system availability, managing blockchain storage growth as institutions scale, balancing computational overhead from cryptographic operations, and ensuring adequate network bandwidth for model parameter exchange [9,441].

In permissioned health care networks, PoA achieves 200-300 TPS and approximately 95% lower energy than PoW, whereas PBFT offers stronger Byzantine resilience at 40%-50% lower throughput [442]. Comparative syntheses show that BCFL improves privacy metrics by 40%-60% over vanilla FL while staying within approximately 3% of centralized accuracy [344,384]. Recent systematic reviews covering literature from 2023-2024 confirm these patterns across diverse health care applications [12,400]. Fully-coupled blockchain-FL designs minimize latency (reduction of 30%-40%) but demand 2-3 times the resources, while semicoupled architectures offer a balanced middle ground [443].

Threats to Validity and Replicability

Information

A crucial aspect of interpreting empirical studies on BCFL involves recognizing their inherent threats to validity. Specifically, researchers must account for the impact of various factors. First, non-independent and identically distributed data and silo imbalance are important aspects, where skewed label and cohort distributions across participating institutions necessitate the reporting of per-site metrics and federated confusion matrices. Second, WAN effects must be meticulously reported for wide-area deployments, including round times, network latency, bandwidth, and specific block/endorsement parameters, to avoid misleading claims based on LAN-only results. Third, attack realism requires results to be reproducible with adaptive rather than static poisoning, along with full disclosure of clipping rules, aggregation mechanisms, and defense strategies. Fourth, from a privacy perspective, privacy budgets must be transparent, demanding the publication of (ϵ, δ) values, sensitivity assumptions, and composition accounting across all training rounds. Fifth, achieving determinism is essential for reproducibility, requiring the release of seeds, exact model/optimizer configurations, client sampling methods, and chaincode/smart contract versions. Finally, accurate compute/power accounting must distinguish between the computational overhead dedicated to model training versus the overhead attributed to blockchain operations, detailing the validator count and hardware thermal design power (TDP). Recent comprehensive reviews have systematically identified

these validity concerns across the literature from 2018-2024 [384,400].

Takeaway

Across clinically meaningful tasks, BCFL achieves near-centralized utility with measurable but manageable overheads when engineered with communication-efficient aggregation and permissioned consensus. Recent empirical evidence from 2024-2025 confirms consistent patterns: accuracy within 2%-3% of centralized baselines, communication overhead reductions of 40%-50%, and successful deployment across 50-200 participating institutions. The primary value additions in health care are auditability, provenance for regulatory processes, and robustness under adversarial and privacy constraints, while the primary bottlenecks are large-scale coordination (≥ 500 nodes) and legacy-system interoperability.

Related Work

Overview

In this section, we comprehensively explore existing research endeavors focusing on integrating BCFL frameworks within health care contexts. Initially, we delve into the corpus of literature dedicated to elucidating the practical applications, methodologies, and outcomes of utilizing blockchain technology in conjunction with FL for health care use cases. In addition, we aim to provide a taxonomy and categorize the existing work based on the insights garnered throughout this paper. To achieve this, we classify the research according to integration architecture (ie, fully coupled, semicoupled, and loosely coupled), blockchain platform, FL type, and data type. Furthermore, we highlight their primary contributions as well as their limitations. Later, we examine existing surveys and reviews focusing on blockchain-assisted FL in health care. This will provide insights into the overall research landscape and help identify any gaps or areas for further exploration.

Literature Review

Samantray and Reddy [444] proposed a hybrid blockchain architecture with quantum key encryption for Healthcare 5.0. Bhasker et al [445] presented a Healthcare 5.0 smart health care system for addressing confidentiality, trust, and compliance standards for safe health monitoring. Bhardwaj et al [428] introduced a privacy-preserving Federated

Blockchain Explainable Artificial Intelligence Optimization (PPFBXAI/O) framework for the integration of blockchain and XAI, and optimization techniques to ensure privacy, traceability, and robustness in FL-based systems. Ali et al [446] presented a ZKP and HE approach for EHR security. Das et al [447] presented a meta-learning approach for improved model generalization.

Chen et al [19] proposed a trustworthy and fair blockchain-based FL framework to address challenges like malicious attacks (model/data poisoning) and free-rider behavior. In another study [448], a quality-aware BCFL with a secure key-sharing mechanism to protect local model parameters and ensure data security was proposed. Mazid et al [436] proposed a blockchain-driven FL framework for secure health care services using IoMT devices. Liang et al [449] proposed a software architecture integrating FL and blockchain to mitigate bias and fairness issues in health care predictive modeling while safeguarding patient privacy. Om Kumar et al [450] introduced a mechanism to reward organizations participating in the FL process, ensuring privacy-preserving model transfer using loosely-coupled integration with the Ethereum blockchain. Moulahi et al [437] integrated FL and blockchain to develop a trusted system for predicting diabetes risk while ensuring data privacy and model integrity.

Ali et al [451] focused on integrating blockchain with FL for secure and decentralized analysis of electronic medical records in precision medicine. Chang et al [442] proposed an integration of adaptive DP and gradient verification-based consensus protocols in a fully-coupled architecture for health care analytics. Lian et al [452] presented a blockchain-based personalized FL system for ensuring security and privacy in IoMT.

Farooq et al [453] developed an automated system for analyzing patients' live data within a fully-coupled architecture, while Zhang et al [454] proposed a blockchain-enabled FL framework for health care data privacy protection. Aich et al [336] introduced a blockchain-assisted FL framework for personal data preservation, and Passerat-Palmbach et al [335] proposed a novel architecture for FL integrated with blockchain within health care systems. A taxonomy of existing research studies, along with additional relevant work, has been compiled in Table 7.

Table 7. Related work on blockchain-assisted FL^a in health care.

Reference	Main contribution	Architecture	Blockchain platform	FL type	Data type	Limitations
Chen et al [19]	Introduces a trustworthy and fair blockchain-based FL framework (FedCFB) to address challenges like malicious attacks (model/data poisoning) and free-rider behavior	Semicoupled	Custom-designed	HFL ^b	Unknown (MNIST)	No discussion on throughput/latency tradeoffs for large-scale FL deployments.
Samantray and Reddy [444]	Hybrid blockchain architecture with quantum key encryption for futuristic health care in smart cities	Loosely coupled	Ethereum	HFL	Medical images and documents	Performance and scalability issues in large-scale implementations.

Reference	Main contribution	Architecture	Blockchain platform	FL type	Data type	Limitations
Bhasker et al [445]	A health care 5.0 smart health care system for addressing confidentiality, trust, and compliance standards for safe health monitoring	Loosely coupled	Unknown	HFL	Wearable devices and sensors	Lack of real-world deployment scenarios and practical validation in actual health care settings.
Bhardwaj and Sumangali [428]	Proposes a privacy-preserving federated blockchain explainable artificial intelligence optimization (PPFBX- AIO) framework, which integrates blockchain, explainable artificial intelligence, and optimization techniques to ensure privacy, traceability, and robustness in FL-based systems	Fully coupled	Unknown	HFL	EHRs ^c	Real-world deployment gaps (ie, does not address practical deployment challenges, such as regulatory compliance with health care standards (HIPAA ^d or GDPR ^e) and integration with existing hospital information systems.
Ali et al [446]	Leverages zero-knowledge proofs and homomorphic encryption for EHR security	Semicoupled	Unknown	HFL	EHRs	Limited empirical validation or real-world testing of the proposed framework.
Das et al [447]	Meta-learning approach for improved model generalization	Semicoupled	Hyperledger Besu	HFL	IoMT ^f data	No real-world implementation (the entire study is simulation-based with no actual deployment and no real medical IoT ^g devices involved), incomplete blockchain implementation, and FL implementation is unclear.
Munusamy and Jothi [344]	Proposes an enhanced privacy-preserving blockchain-enabled federated learning (EPP-BCFL) framework that integrates blockchain with hybrid privacy mechanisms and intelligent aggregation strategies for secure EHR	Semicoupled	Hyperledger Fabric	HFL	Medical imaging data (CIFAR-10)	Evaluation limited to CIFAR-10 rather than clinical datasets.
Lo et al [455]	Proposes a BCFL ^h architecture to enable accountability in FL systems.	Loosely coupled	Ethereum	HFL	Medical imaging data (COVID-19 CT ⁱ)	Lack of real-world deployment analysis.
Kumar et al [448]	Proposes a quality-aware BCFL with a secure key-sharing mechanism to protect local model parameters and ensure data security	Loosely coupled	Unknown	HFL	Unknown	Limited scale and real-world testing (eg, not tested in actual hospital environments, no real health care institutions involved, etc).
Mazid et al [436]	Proposes a blockchain-driven FL framework for secure health care services using IoMT devices	Loosely coupled	Unknown	HFL	Medical imaging (colon pathology, breast tumor)	Validated only through simulations, using benchmark datasets (2D colon pathology, breast tumor, and CIFAR-10). There is no real-world hospital or IoMT deployment, which limits conclusions.
Liang et al [449]	Software architecture integrating FL and blockchain to tackle bias and fairness issues in health care predictive modeling while safeguarding patient privacy	Semicoupled	Rahasak	Unknown	Unknown	Limited real-world validation. This study was conducted in a simulated environment with only 5 simulated medical centers rather than actual health care institutions. This significantly limits the generalizability of findings to real-world health care settings.
Om Kumar et al [450]	Introduces a mechanism to reward organizations participating in the FL process, ensuring privacy-preserving model transfer between users and organizations using blockchain	Loosely coupled	Ethereum	HFL	Medical imaging data (COVID-19 CT)	Not explicitly stated.

Reference	Main contribution	Architecture	Blockchain platform	FL type	Data type	Limitations
Moulahi et al [437]	Integrates FL and blockchain technology to develop a trusted system for predicting diabetes risk while ensuring data privacy and model integrity	Semicoupled	Ethereum	HFL	Sensor data (IoT)	Not explicitly stated.
Ali et al [451]	Integrates blockchain with FL to enable secure and decentralized analysis of EMRs in precision medicine	Loosely coupled	Ethereum, Hyperledger Fabric (simulation)	HFL	EMR	The paper appears to be primarily theoretical and simulation-based without actual deployment in real health care settings (eg, there is no evidence of testing with actual health care institutions or real EMR) and limited experimental validation (eg, no specific dataset characteristics are provided).
Chang et al [442]	Integrates adaptive differential privacy and gradient verification-based consensus protocols	Fully coupled	Ethereum	HFL/VFL ^j	IoMT sensor data	Scalability challenges, increased complexity, potential computational overhead, and the need for further validation across diverse medical conditions and datasets.
Lian et al [452]	Blockchain-based personalized FL system to address security and privacy concerns in IoMT	Fully coupled	Unknown (consortium PoS ^k blockchain)	VFL	IoMT sensor data (Fashion-MNIST)	Limited experimental validation (eg, only simulated experiments were used rather than real-world deployment, tested on Fashion-MNIST and CIFAR-10 [image classification datasets]; no actual medical data, etc).
Farooq et al [453]	Develops an automated system for analyzing patients' live data	Fully coupled	Ethereum	HFL	IoMT sensor data	Limited empirical validation or real-world testing of the proposed framework.
Zhang et al [454]	Proposes a BCFL framework for health care data privacy protection	Fully coupled	Unknown (conceptual)	HFL	EHR (MNIST)	Theoretical model only, not supported via experimental implementations.
Aich et al [336]	Proposes a blockchain-assisted FL framework for personal data preserving	Loosely coupled	Unknown (conceptual)	— ^l	No data	Reliance on conceptual assumptions without real-world application.
Passerat-Palmbach et al [335]	Proposes a novel architecture for FL integrated with blockchain within a health care system	Loosely coupled	Ethereum	—	No data	Not explicitly stated.
Rahman et al [438]	Proposes a BCFL framework for COVID-19 applications to classify IoHT ^m data	Loosely coupled	Ethereum	FL type	Sensor data (IoMT)	Not explicitly stated.
Singh et al [456]	Integrates blockchain technology with FL to enhance privacy preservation and scalability in health care data management	Fully coupled	Unknown	Unknown	Sensor data (IoT)	Theoretical model only, not supported via experimental implementations.
Nguyen et al [457]	Proposes a new blockchain-enabled FL-based generative adversarial network framework for secure COVID-19 data analytics	Semicoupled	Unknown (conceptual)	HFL	Medical imaging data (COVID-19 CT)	The blockchain model is conceptual, and a real-world implementation was not reported.
Liu et al [458]	Proposes a framework of blockchain-empowered FL in health care-based cyber-physical systems	Fully coupled	Ethereum	HFL	EHR (MNIST HAM10000)	Not explicitly stated.
Otoum et al [459]	Proposes a novel solution for revolutionizing health care systems by considering concepts like distributivity, self-learnability, and autonomy.	—	Unknown (conceptual)	Unknown	No data	Only introduces a theoretical framework without an empirical validation.

Reference	Main contribution	Architecture	Blockchain platform	FL type	Data type	Limitations
Kumar et al [433]	Blockchain-empowered method to detect patterns of COVID-19 from lung CT scans	Fully coupled	Unknown	HFL	Medical imaging data (COVID-19 CT)	The paper does not extensively discuss the generalization capabilities of the proposed model to handle variations in COVID-19 manifestations across different patients.
Durga and Poovammal [460]	A concise review of BCFL in health care, concepts, and taxonomy	—	Unknown	Unknown	Unknown	The article is very brief and does not cover all concepts.
Lakhan et al [461]	Proposes a FL-based blockchain-enabled task scheduling (FLBETS) framework with different dynamic heuristics for health care applications	Loosely coupled	Unknown	Unknown	Sensor data (IoMT)	Dynamic and run-time unknown attacks against IoMT were not considered in this work.
Samuel et al [462]	Introduces FedMedChain as a BCFL framework for medical data privacy preservation	Loosely coupled	Unknown	Unknown	Sensor data (Unknown)	Not explicitly stated.
Yang and Xing [463]	Introduces a privacy protection framework for medical data using blockchain and FL for secure and auditable data sharing among medical institutions using a secure aggregation scheme based on homomorphic encryption	Loosely coupled	Ethereum	HFL	EHR (MNIST different datasets)	Not explicitly stated.

^aFL: federated learning.

^bHFL: horizontal federated learning.

^cEHRs: electronic health records.

^dHIPAA: Health Insurance Portability and Accountability Act.

^eGDPR: General Data Protection Regulation.

^fIoMT: Internet of Medical Things.

^gIoT: Internet of Things.

^hBCFL: blockchain-based federated learning.

ⁱCT: computed tomography.

^jVFL: vertical federated learning.

^kPoS: proof of stake.

^lNot applicable/not available.

^mIoHT: Internet of Healthcare Things.

Existing Surveys

To the best of our knowledge, comprehensive surveys or reviews focusing on the integration of blockchain and FL for health care use cases are scarce. While individual studies have explored the potential of each technology independently within health care settings, there is a notable lack of resources delving into the synergistic benefits and challenges of combining blockchain's immutable ledger capabilities with FL's decentralized model training approach.

Ngoupayou Limbepe et al [12] presented a taxonomy of FL-based privacy mechanisms categorized into privacy-enhancing technologies and hybrid techniques. This survey integrates privacy-enhancing technologies with blockchain in FL frameworks for smart health care systems. Noteworthy initial explorations, such as those conducted by Myrzashova et al [13] and Nguyen et al [464], offer valuable insights but often lack a broader perspective. Myrzashova et al [13], for instance, analyzed the advantages and disadvantages of BCFL integration in health care, but they overlooked the importance of a data type taxonomy. Understanding the diverse medical data types (eg, genomics and imaging) used in health care ML

is crucial, as different data may have varying security and privacy requirements. Similarly, Nguyen et al [464] introduced a new conceptual architecture that integrates blockchain and AI for combating the COVID-19 pandemic. While offering valuable insights into addressing specific challenges posed by the pandemic, its scope is limited to COVID-19 and related data, lacking a broader analysis of the integration's potential for various health care use cases beyond this specific context. Hemdan et al [465] examined the convergence of digital twin technology, blockchain, and FL in the medical field, with a specific focus on their technical architecture and real-world applications. Orabi et al [400] presented a literature review of BCFL applications in health care for protecting sensitive data. This paper investigated how integrating FL with blockchain can enhance its security, performance, and reliability.

In contrast to these existing reports, this tutorial offers a more comprehensive perspective. We present a taxonomy of medical data used for ML, providing a foundational understanding of the diverse data types relevant to this integration. Furthermore, we unveil an innovative architecture meticulously designed for the seamless integration of blockchain and

FL within health care systems, addressing the need for secure and privacy-preserving health care analytics.

Future Research Directions

Overview

The integration of FL and blockchain in health care introduces a transformative paradigm for secure, privacy-preserving, and collaborative medical AI systems. Despite notable theoretical advances, several research frontiers remain underexplored. These can be broadly categorized into 4 interrelated areas: cryptographic foundations and quantum-resilient privacy, scalable and interoperable infrastructure, health care-specific consensus and incentivization, and full-stack integration with regulatory automation.

Cryptographic Foundations and Quantum-Resilient Privacy

A core requirement for the secure deployment of BCFL systems in health care is the development of advanced cryptographic mechanisms that ensure long-term privacy, data integrity, and resilience against quantum adversaries. Postquantum cryptographic primitives (such as lattice-based schemes like CRYSTALS-Kyber and Dilithium, and hash-based schemes like SPHINCS+) must be integrated into the BCFL stack to secure signatures and encryption layers [466]. In parallel, ZKPs and zero-knowledge virtual machines offer promising approaches to verifiably audit FL operations and regulatory compliance without exposing raw medical data. Furthermore, HE schemes, particularly multikey variants of the CKKS (Cheon-KimKim-Song) cryptosystem [467], enable secure aggregation of encrypted model parameters from multiple health care institutions without revealing individual contributions. The substantial computational overhead of such operations can be alleviated through specialized hardware accelerators, notably smart network interface cards, which offload cryptographic computations to dedicated processing units, thereby improving efficiency and scalability [468]. Complementarily, DP mechanisms require refinement to handle medical-specific feature types, with research needed into adaptive noise strategies and budget allocation tailored to data sensitivity. Together, these innovations will enable secure, auditable, and privacy-preserving collaborative learning in health care environments.

Scalable and Interoperable BCFL Infrastructure

As clinical systems generate increasingly voluminous and heterogeneous data, BCFL infrastructure must address throughput, latency, and interoperability challenges to support real-time learning and inference [401,439]. Health care-specific sharding architectures (such as parallel blockchains for EHRs, medical imaging, and genomics) can significantly improve throughput by distributing model updates across application domains. Complementary to this, layer-2 scaling solutions, including rollups [469] and state channels, offer reductions in transaction costs and ledger bloat, making

frequent model updates feasible without congesting the blockchain [470]. Additionally, cross-chain interoperability mechanisms, such as those based on the Cosmos IBC protocol or Polkadot's relay chain model, are essential for enabling collaboration among health care institutions operating on heterogeneous blockchain platforms. Moreover, edge-centric FL will become increasingly important as IoMT and wearable devices proliferate. Furthermore, split learning and energy-efficient blockchain clients will be crucial to bring BCFL capabilities to constrained edge nodes while preserving security guarantees. These advancements will enable a scalable and interoperable ecosystem capable of supporting global health care collaborations.

Health Care-Specific Consensus and Incentive Mechanisms

Generic blockchain consensus protocols are ill-suited for the privacy, latency, and regulatory demands of health care. There is a growing need to design health care-oriented consensus protocols, such as medical and practical BFT [471], which can minimize communication overhead and incorporate privacy-aware authorization and medical rule validation into the consensus process. Similarly, reputation-based BFT [472] can ensure the credibility of participating institutions and practitioners, dynamically adjusting voting power based on behavior and contribution history. To sustain active participation in FL processes, especially among resource-constrained or data-rich stakeholders, incentive mechanisms must be tailored to health care environments. The proof-of-federated-work paradigm introduces an innovative strategy to quantify participant contributions using metrics like local accuracy, data diversity, and compliance adherence [473]. These are integrated into token-based or hybrid compensation schemes, further reinforced by game-theoretic models that optimize incentives based on Nash equilibrium to deter free-riding and encourage high-quality model updates. Such mechanisms are foundational to the long-term viability of decentralized health care learning networks.

System Integration, Compliance Automation, and Real-World Translation

For BCFL frameworks to be deployed at scale, they must integrate seamlessly with health care systems, satisfy regulatory requirements, and maintain usability in real-time clinical contexts. Smart contracts should evolve to support automated, upgradeable compliance verification that is capable of adapting to dynamic legal frameworks such as HIPAA, GDPR, and FDA AI guidelines [474]. By incorporating ZKP-based attestations, institutions can demonstrate compliance without revealing sensitive patient-level operations [440]. Simultaneously, embedding explainable AI techniques, such as SHAP values and attention heatmaps, into the FL pipeline is essential to ensure clinician trust and support regulatory transparency [475]. Algorithmically, innovations in personalized FL, multitask learning (eg, MOCHA [476]), and community-based learning [477] can help address patient heterogeneity and improve predictive power in distributed environments. Real-time FL

capabilities, triggered by event-driven smart contracts (eg, emergency alerts), are crucial for responsive applications like ICU triage and chronic condition monitoring [432]. To ensure long-term sustainability, quantum-resistant blockchain architectures should be explored using crypto-agile protocols and hybrid classical/postquantum stacks. These systems must also support interoperability, modular compliance, and secure cross-border data flows, forming the backbone of globally federated, privacy-aware health care AI infrastructure.

Conclusion

This tutorial introduced a comprehensive, clinically oriented, and compliance-aware framework integrating FL and blockchain for secure and privacy-preserving health care analytics. We demonstrated how FL enables decentralized model training across health care institutions while maintaining data locality and how blockchain enhances trust, integrity, and auditability through immutable ledgers and decentralized consensus mechanisms. Our key contributions include the following: (1) a systematic taxonomy of diverse medical data types and their FL requirements; (2) three novel

integration architectures (fully coupled, semicoupled, and loosely coupled) with rigorous analysis of security, scalability, and regulatory compliance tradeoffs; (3) comprehensive security analysis identifying health care-specific vulnerabilities and mitigation strategies using advanced cryptographic techniques, including ZKPs, HE, and DP; and (4) a practical regulatory compliance framework addressing HIPAA, GDPR, and FDA guidelines for AI/ML-based medical devices. We validated BCFL effectiveness across critical health care applications, including disease prediction, medical imaging analysis, patient monitoring, and drug discovery. Looking ahead, crucial research frontiers involve quantum-resilient cryptography, scalable interoperable infrastructure, health care-specific consensus mechanisms, and automated compliance frameworks. This tutorial provides a foundational reference for developing trustworthy and patient-centric AI systems in health care. By integrating blockchain and FL, these systems can transform health care delivery while safeguarding privacy, ensuring regulatory compliance, and ultimately driving improved patient outcomes and accelerating medical discoveries in an increasingly connected health care ecosystem.

Acknowledgments

The authors would like to thank the anonymous reviewers and the academic editor for their constructive comments, which helped improve the quality and clarity of this tutorial. Artificial intelligence was used for refining, correcting, and editing the manuscript to improve language clarity.

Funding

This research was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC).

Data Availability

No new datasets were generated or analyzed during this study. All information discussed in this tutorial is derived from previously published literature and publicly available sources.

Authors' Contributions

Conceptualization: YS

Funding acquisition: AH, DM

Investigation: YS

Methodology: YS, YB

Supervision: YS, AH

Writing – original draft: YS, YB, OAD

Writing – review & editing: YS, YB

Conflicts of Interest

None declared.

References

1. Ometov A, Shubina V, Klus L, et al. A survey on wearable technology: history, state-of-the-art and current challenges. *Computer Networks*. Jul 2021;193:108074. [doi: [10.1016/j.comnet.2021.108074](https://doi.org/10.1016/j.comnet.2021.108074)]
2. Kang HS, Exworthy M. Wearing the future-wearables to empower users to take greater responsibility for their health and care: scoping review. *JMIR Mhealth Uhealth*. Jul 13, 2022;10(7):e35684. [doi: [10.2196/35684](https://doi.org/10.2196/35684)] [Medline: [35830222](https://pubmed.ncbi.nlm.nih.gov/35830222/)]
3. Wu M. Wearable technology applications in healthcare: a literature review. *Online J Nurs Inform*. 2019;23(3). URL: <https://www.proquest.com/openview/6c96964dfb83ca06895f330233831a50/1?pq-origsite=gscholar&cbl=2034896> [Accessed 2026-06-01]
4. Zhang C, Xie Y, Bai H, Yu B, Li W, Gao Y. A survey on federated learning. *Knowl Based Syst*. Mar 2021;216:106775. [doi: [10.1016/j.knosys.2021.106775](https://doi.org/10.1016/j.knosys.2021.106775)]

5. Babar M, Qureshi B, Koubaa A. Review on federated learning for digital transformation in healthcare through big data analytics. *Future Generation Computer Systems*. Nov 2024;160:14-28. [doi: [10.1016/j.future.2024.05.046](https://doi.org/10.1016/j.future.2024.05.046)]
6. Fang M, Cao X, Jia J, Gong N. Local model poisoning attacks to byzantine-robust federated learning. Presented at: 29th USENIX Security Symposium; Aug 12-14, 2020; Boston, MA, USA. URL: <https://www.usenix.org/system/files/sec20-fang.pdf> [Accessed 2026-05-07]
7. Kumar KN, Mohan CK, Cenkeramaddi LR, Awasthi N. Minimal data poisoning attack in federated learning for medical image classification: an attacker perspective. *Artif Intell Med*. Jan 2025;159:103024. [doi: [10.1016/j.artmed.2024.103024](https://doi.org/10.1016/j.artmed.2024.103024)] [Medline: [39591879](https://pubmed.ncbi.nlm.nih.gov/39591879/)]
8. Bouacida N, Mohapatra P. Vulnerabilities in federated learning. *IEEE Access*. 2021;9:63229-63249. [doi: [10.1109/ACCESS.2021.3075203](https://doi.org/10.1109/ACCESS.2021.3075203)]
9. Cai Z, Chen J, Fan Y, Zheng Z, Li K. Blockchain-empowered federated learning: benefits, challenges, and solutions. *IEEE Trans Big Data*. Feb 13, 2025;11(5):2244-2263. [doi: [10.1109/TBDATA.2025.3541560](https://doi.org/10.1109/TBDATA.2025.3541560)]
10. Abbas SR, Abbas Z, Zahir A, Lee SW. Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration. *Healthcare (Basel)*. Dec 22, 2024;12(24):2587. [doi: [10.3390/healthcare12242587](https://doi.org/10.3390/healthcare12242587)] [Medline: [39766014](https://pubmed.ncbi.nlm.nih.gov/39766014/)]
11. Cheng H, Qu Y, Liu W, Gao L, Zhu T. Decentralized federated learning for private smart healthcare: a survey. *Mathematics*. 2025;13(8):1296. [doi: [10.3390/math13081296](https://doi.org/10.3390/math13081296)]
12. Ngoupayou Limbepe Z, Gai K, Yu J. Blockchain-based privacy-enhancing federated learning in smart healthcare: a survey. *Blockchains*. 2025;3(1):1. [doi: [10.3390/blockchains3010001](https://doi.org/10.3390/blockchains3010001)]
13. Myrzashova R, Alsamhi SH, Shvetsov AV, Hawbani A, Wei X. Blockchain meets federated learning in healthcare: a systematic review with challenges and opportunities. *IEEE Internet Things J*. 2023;10(16):14418-14437. [doi: [10.1109/JIOT.2023.3263598](https://doi.org/10.1109/JIOT.2023.3263598)]
14. Datta P, Namin AS, Chatterjee M. A survey of privacy concerns in wearable devices. Presented at: 2018 IEEE International Conference on Big Data (Big Data); Dec 10-13, 2018; Seattle, WA, USA. [doi: [10.1109/BigData.2018.8622110](https://doi.org/10.1109/BigData.2018.8622110)]
15. Qayyum A, Qadir J, Bilal M, Al-Fuqaha A. Secure and robust machine learning for healthcare: a survey. *IEEE Rev Biomed Eng*. 2021;14:156-180. [doi: [10.1109/RBME.2020.3013489](https://doi.org/10.1109/RBME.2020.3013489)] [Medline: [32746371](https://pubmed.ncbi.nlm.nih.gov/32746371/)]
16. Cilliers L. Wearable devices in healthcare: privacy and information security issues. *Health Inf Manag*. 2020;49(2-3):150-156. [doi: [10.1177/1833358319851684](https://doi.org/10.1177/1833358319851684)] [Medline: [31146589](https://pubmed.ncbi.nlm.nih.gov/31146589/)]
17. Lyu L, Yu H, Ma X, et al. Privacy and robustness in federated learning: attacks and defenses. *IEEE Trans Neural Netw Learning Syst*. 2024;35(7):8726-8746. [doi: [10.1109/TNNLS.2022.3216981](https://doi.org/10.1109/TNNLS.2022.3216981)]
18. Ye H, Liang L, Li GY. Decentralized federated learning with unreliable communications. *IEEE J Sel Top Signal Process*. 2022;16(3):487-500. [doi: [10.1109/JSTSP.2022.3152445](https://doi.org/10.1109/JSTSP.2022.3152445)]
19. Chen L, Zhao D, Tao L, et al. A credible and fair federated learning framework based on blockchain. *IEEE Trans Artif Intell*. 2024;6(2):301-316. [doi: [10.1109/TAI.2024.3355362](https://doi.org/10.1109/TAI.2024.3355362)]
20. Gupta M, Kumar M, Dhir R. Unleashing the prospective of blockchain-federated learning fusion for IoT security: a comprehensive review. *Computer Science Review*. Nov 2024;54:100685. [doi: [10.1016/j.cosrev.2024.100685](https://doi.org/10.1016/j.cosrev.2024.100685)]
21. Qu Y, Uddin MP, Gan C, Xiang Y, Gao L, Yearwood J. Blockchain-enabled federated learning: a survey. *ACM Comput Surv*. Apr 30, 2023;55(4):1-35. [doi: [10.1145/3524104](https://doi.org/10.1145/3524104)]
22. Zhu J, Cao J, Saxena D, Jiang S, Ferradi H. Blockchain-empowered federated learning: challenges, solutions, and future directions. *ACM Comput Surv*. Nov 30, 2023;55(11):1-31. [doi: [10.1145/3570953](https://doi.org/10.1145/3570953)]
23. Qammar A, Karim A, Ning H, Ding J. Securing federated learning with blockchain: a systematic literature review. *Artif Intell Rev*. 2023;56(5):3951-3985. [doi: [10.1007/s10462-022-10271-9](https://doi.org/10.1007/s10462-022-10271-9)] [Medline: [36160367](https://pubmed.ncbi.nlm.nih.gov/36160367/)]
24. Ramakrishnaiah Y, Macesic N, Webb GI, Peleg AY, Tyagi S. EHR-ML: a data-driven framework for designing machine learning applications with electronic health records. *Int J Med Inform*. Apr 2025;196:105816. [doi: [10.1016/j.ijmedinf.2025.105816](https://doi.org/10.1016/j.ijmedinf.2025.105816)] [Medline: [39891983](https://pubmed.ncbi.nlm.nih.gov/39891983/)]
25. Shen Y, Yu J, Zhou J, Hu G. Twenty-five years of evolution and hurdles in electronic health records and interoperability in medical research: comprehensive review. *J Med Internet Res*. Jan 9, 2025;27:e59024. [doi: [10.2196/59024](https://doi.org/10.2196/59024)] [Medline: [39787599](https://pubmed.ncbi.nlm.nih.gov/39787599/)]
26. Nowrozy R, Ahmed K, Kayes ASM, Wang H, McIntosh TR. Privacy preservation of electronic health records in the modern era: a systematic survey. *ACM Comput Surv*. Aug 31, 2024;56(8):1-37. [doi: [10.1145/3653297](https://doi.org/10.1145/3653297)]
27. Arbet J, Brokamp C, Meinzen-Derr J, Trinkley KE, Spratt HM. Lessons and tips for designing a machine learning study using EHR data. *J Clin Trans Sci*. 2021;5(1):e21. [doi: [10.1017/cts.2020.513](https://doi.org/10.1017/cts.2020.513)]
28. Wu H, Yamal JM, Yaseen A, Maroufy V. *Statistics and Machine Learning Methods for EHR Data: From Data Extraction to Data Analytics*. CRC Press; 2020. [doi: [10.1201/9781003030003](https://doi.org/10.1201/9781003030003)]

29. Johnston SS, Morton JM, Kalsekar I, Ammann EM, Hsiao CW, Reys J. Using machine learning applied to real-world healthcare data for predictive analytics: an applied example in bariatric surgery. *Value Health*. May 2019;22(5):580-586. [doi: [10.1016/j.jval.2019.01.011](https://doi.org/10.1016/j.jval.2019.01.011)] [Medline: [31104738](https://pubmed.ncbi.nlm.nih.gov/31104738/)]
30. Muniasamy A, Tabassam S, Hussain MA, Sultana H, Muniasamy V, Bhatnagar R. Deep learning for predictive analytics in healthcare. In: Hassanien A, Azar A, Gaber T, Bhatnagar R, Tolba M, editors. *The International Conference on Advanced Machine Learning Technologies and Applications (AMLT2019) AMLTA 2019 Advances in Intelligent Systems and Computing*. Springer; 2020:32-42. [doi: [10.1007/978-3-030-14118-9_4](https://doi.org/10.1007/978-3-030-14118-9_4)]
31. Singh P, Singh N, Singh KK, Singh A. Diagnosing of disease using machine learning. In: Singh KK, Elhoseny M, Singh A, Elngar AA, editors. *Machine Learning and the Internet of Medical Things in Healthcare*. Academic Press; 2021:89-111. [doi: [10.1016/B978-0-12-821229-5.00003-3](https://doi.org/10.1016/B978-0-12-821229-5.00003-3)]
32. Ahsan MM, Luna SA, Siddique Z. Machine-learning-based disease diagnosis: a comprehensive review. *Healthcare (Basel)*. Mar 15, 2022;10(3):541. [doi: [10.3390/healthcare10030541](https://doi.org/10.3390/healthcare10030541)] [Medline: [35327018](https://pubmed.ncbi.nlm.nih.gov/35327018/)]
33. Komal Kumar N, Vigneswari D. A drug recommendation system for multi-disease in health care using machine learning. In: Hura GS, Singh AK, Siong Hoe L, editors. *Advances in Communication and Computational Technology ICACCT 2019 Lecture Notes in Electrical Engineering*. Springer; 2021:1-12. [doi: [10.1007/978-981-15-5341-7_1](https://doi.org/10.1007/978-981-15-5341-7_1)]
34. Abhisheka B, Biswas SK, Purkayastha B, Das D, Escargueil A. Recent trend in medical imaging modalities and their applications in disease diagnosis: a review. *Multimed Tools Appl*. 2023;83(14):43035-43070. [doi: [10.1007/s11042-023-17326-1](https://doi.org/10.1007/s11042-023-17326-1)]
35. Lalitha S, Sanjana T, Bhavana H, Bhan I, Harshith G. Medical imaging modalities and different image processing techniques: state of the art review. In: Shinde SV, Mahalle PN, Bendre V, Castillo O, editors. *Disruptive Developments in Biomedical Applications*. CRC Press; 2022:17-36. [doi: [10.1201/9781003272694-3](https://doi.org/10.1201/9781003272694-3)]
36. Santhi K. A survey on medical imaging techniques and applications. *J Innov Image Process*. 2022;4(3):173-182. [doi: [10.36548/jiip.2022.3.005](https://doi.org/10.36548/jiip.2022.3.005)]
37. Mustapha MT, Uzun B, Ozsahin DU, Ozsahin I. A comparative study of x-ray based medical imaging devices. In: Ozsahin I, OzsahinDU, Uzun B, editors. *Applications of Multi-Criteria Decision-Making Theories in Healthcare and Biomedical Engineering*. Academic Press; 2021:163-180. [doi: [10.1016/B978-0-12-824086-1.00011-6](https://doi.org/10.1016/B978-0-12-824086-1.00011-6)]
38. Withers PJ, Bouman C, Carmignato S, et al. X-ray computed tomography. *Nat Rev Methods Primers*. 2021;1(1):18. [doi: [10.1038/s43586-021-00015-4](https://doi.org/10.1038/s43586-021-00015-4)]
39. De Pietro S, Di Martino G, Caroprese M, et al. The role of MRI in radiotherapy planning: a narrative review “from head to toe”. *Insights Imaging*. Oct 23, 2024;15(1):255. [doi: [10.1186/s13244-024-01799-1](https://doi.org/10.1186/s13244-024-01799-1)] [Medline: [39441404](https://pubmed.ncbi.nlm.nih.gov/39441404/)]
40. Avola D, Cinque L, Fagioli A, Foresti G, Mecca A. Ultrasound medical imaging techniques. *ACM Comput Surv*. Apr 30, 2022;54(3):1-38. [doi: [10.1145/3447243](https://doi.org/10.1145/3447243)]
41. Cullen A, O'Connell M. Tutorial 14: introduction to nuclear medicine. In: Redmond C, Lee M, editors. *Tutorials in Diagnostic Radiology for Medical Students*. Springer; 2020:225-233. [doi: [10.1007/978-3-030-31893-2_14](https://doi.org/10.1007/978-3-030-31893-2_14)]
42. Wernick MN, Aarsvold JN. *Emission Tomography: The Fundamentals of PET and SPECT*. Academic Press; 2004. ISBN: 9780127444826
43. Jones AK, Balter S, Rauch P, Wagner LK. Medical imaging using ionizing radiation: optimization of dose and image quality in fluoroscopy. *Med Phys*. Jan 2014;41(1):014301. [doi: [10.1118/1.4835495](https://doi.org/10.1118/1.4835495)] [Medline: [24387534](https://pubmed.ncbi.nlm.nih.gov/24387534/)]
44. Ulrich H, Kock-Schoppenhauer AK, Deppenwiese N, et al. Understanding the nature of metadata: systematic review. *J Med Internet Res*. Jan 11, 2022;24(1):e25440. [doi: [10.2196/25440](https://doi.org/10.2196/25440)] [Medline: [35014967](https://pubmed.ncbi.nlm.nih.gov/35014967/)]
45. Bhuiyan MN, Rahman MM, Billah MM, Saha D. Internet of things (IoT): a review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet Things J*. 2021;8(13):10474-10498. [doi: [10.1109/JIOT.2021.3062630](https://doi.org/10.1109/JIOT.2021.3062630)]
46. Larobina M. Thirty years of the DICOM standard. *Tomography*. Oct 6, 2023;9(5):1829-1838. [doi: [10.3390/tomography9050145](https://doi.org/10.3390/tomography9050145)] [Medline: [37888737](https://pubmed.ncbi.nlm.nih.gov/37888737/)]
47. Wang J, Wang S, Zhang Y. Deep learning on medical image analysis. *CAAI Trans on Intel Tech*. Feb 2025;10(1):1-35. [doi: [10.1049/cit2.12356](https://doi.org/10.1049/cit2.12356)]
48. Rana M, Bhushan M. Machine learning and deep learning approach for medical image analysis: diagnosis to detection. *Multimed Tools Appl*. Jul 2023;82(17):26731-26769. [doi: [10.1007/s11042-022-14305-w](https://doi.org/10.1007/s11042-022-14305-w)]
49. Jeyaraj PR, Samuel Nadar ER. Computer-assisted medical image classification for early diagnosis of oral cancer employing deep learning algorithm. *J Cancer Res Clin Oncol*. Apr 2019;145(4):829-837. [doi: [10.1007/s00432-018-02834-7](https://doi.org/10.1007/s00432-018-02834-7)] [Medline: [30603908](https://pubmed.ncbi.nlm.nih.gov/30603908/)]
50. Echle A, Rindtorff NT, Brinker TJ, Luedde T, Pearson AT, Kather JN. Deep learning in cancer pathology: a new generation of clinical biomarkers. *Br J Cancer*. Feb 2021;124(4):686-696. [doi: [10.1038/s41416-020-01122-x](https://doi.org/10.1038/s41416-020-01122-x)] [Medline: [33204028](https://pubmed.ncbi.nlm.nih.gov/33204028/)]

51. Savadjiev P, Chong J, Dohan A, et al. Image-based biomarkers for solid tumor quantification. *Eur Radiol*. Oct 2019;29(10):5431-5440. [doi: [10.1007/s00330-019-06169-w](https://doi.org/10.1007/s00330-019-06169-w)] [Medline: [30963275](https://pubmed.ncbi.nlm.nih.gov/30963275/)]
52. Xu Y, Hosny A, Zeleznik R, et al. Deep learning predicts lung cancer treatment response from serial medical imaging. *Clin Cancer Res*. Jun 1, 2019;25(11):3266-3275. [doi: [10.1158/1078-0432.CCR-18-2495](https://doi.org/10.1158/1078-0432.CCR-18-2495)] [Medline: [31010833](https://pubmed.ncbi.nlm.nih.gov/31010833/)]
53. Ahishakiye E, Van Gijzen MB, Tumwiine J, Wario R, Obungoloch J. A survey on deep learning in medical image reconstruction. *Intelligent Medicine*. Sep 2021;1(3):118-127. [doi: [10.1016/j.imed.2021.03.003](https://doi.org/10.1016/j.imed.2021.03.003)]
54. Vamathevan J, Clark D, Czodrowski P, et al. Applications of machine learning in drug discovery and development. *Nat Rev Drug Discov*. Jun 2019;18(6):463-477. [doi: [10.1038/s41573-019-0024-5](https://doi.org/10.1038/s41573-019-0024-5)] [Medline: [30976107](https://pubmed.ncbi.nlm.nih.gov/30976107/)]
55. Ginsburg GS, Willard HF. Genomic and personalized medicine: foundations and applications. *Transl Res*. Dec 2009;154(6):277-287. [doi: [10.1016/j.trsl.2009.09.005](https://doi.org/10.1016/j.trsl.2009.09.005)] [Medline: [19931193](https://pubmed.ncbi.nlm.nih.gov/19931193/)]
56. Chen YM, Hsiao TH, Lin CH, Fann YC. Unlocking precision medicine: clinical applications of integrating health records, genetics, and immunology through artificial intelligence. *J Biomed Sci*. Feb 7, 2025;32(1):16. [doi: [10.1186/s12929-024-01110-w](https://doi.org/10.1186/s12929-024-01110-w)] [Medline: [39915780](https://pubmed.ncbi.nlm.nih.gov/39915780/)]
57. Gupta S, Janu N, Nawal M, Goswami A. Genomics and machine learning: ML approaches, future directions and challenges in genomics. In: Choudhary S, Kumar S, Gowroju S, Gulhane M, Sri Lakshmi R, editors. *Genomics at the Nexus of AI, Computer Vision, and Machine Learning*. 2025:437-457. [doi: [10.1002/9781394268832.ch20](https://doi.org/10.1002/9781394268832.ch20)]
58. Suissa JS, De La Cerda GY, Graber LC, et al. Data-driven guidelines for phylogenomic analyses using SNP data. *Appl Plant Sci*. 2024;12(6):e11611. [doi: [10.1002/aps3.11611](https://doi.org/10.1002/aps3.11611)] [Medline: [39628540](https://pubmed.ncbi.nlm.nih.gov/39628540/)]
59. Hollox EJ, Zuccherato LW, Tucci S. Genome structural variation in human evolution. *Trends Genet*. Jan 2022;38(1):45-58. [doi: [10.1016/j.tig.2021.06.015](https://doi.org/10.1016/j.tig.2021.06.015)] [Medline: [34284881](https://pubmed.ncbi.nlm.nih.gov/34284881/)]
60. Audic S, Claverie JM. The significance of digital gene expression profiles. *Genome Res*. Oct 1997;7(10):986-995. [doi: [10.1101/gr.7.10.986](https://doi.org/10.1101/gr.7.10.986)] [Medline: [9331369](https://pubmed.ncbi.nlm.nih.gov/9331369/)]
61. Dai W, Qiao X, Fang Y, et al. Epigenetics-targeted drugs: current paradigms and future challenges. *Sig Transduct Target Ther*. 2024;9(1):332. [doi: [10.1038/s41392-024-02039-0](https://doi.org/10.1038/s41392-024-02039-0)]
62. Schmitz MJ, Bashar A, Soman V, et al. Leveraging diverse genomic data to guide equitable carrier screening: Insights from gnomAD v4.1.0. *Am J Hum Genet*. Jan 2, 2025;112(1):181-195. [doi: [10.1016/j.ajhg.2024.11.004](https://doi.org/10.1016/j.ajhg.2024.11.004)] [Medline: [39615480](https://pubmed.ncbi.nlm.nih.gov/39615480/)]
63. Gulamali FF, Sawant AS, Nadkarni GN. Machine learning for risk stratification in kidney disease. *Curr Opin Nephrol Hypertens*. Nov 1, 2022;31(6):548-552. [doi: [10.1097/MNH.0000000000000832](https://doi.org/10.1097/MNH.0000000000000832)] [Medline: [36004937](https://pubmed.ncbi.nlm.nih.gov/36004937/)]
64. Jamalnia M, Weiskirchen R. Advances in personalized medicine: translating genomic insights into targeted therapies for cancer treatment. *Ann Transl Med*. Apr 30, 2025;13(2):18. [doi: [10.21037/atm-25-34](https://doi.org/10.21037/atm-25-34)] [Medline: [40438512](https://pubmed.ncbi.nlm.nih.gov/40438512/)]
65. Mani S, Lalani SR, Pammi M. Genomics and multiomics in the age of precision medicine. *Pediatr Res*. Mar 2025;97(4):1399-1410. [doi: [10.1038/s41390-025-04021-0](https://doi.org/10.1038/s41390-025-04021-0)] [Medline: [40185865](https://pubmed.ncbi.nlm.nih.gov/40185865/)]
66. Vadapalli S, Abdelhalim H, Zeeshan S, Ahmed Z. Artificial intelligence and machine learning approaches using gene expression and variant data for personalized medicine. *Brief Bioinform*. Sep 20, 2022;23(5):bbac191. [doi: [10.1093/bib/bbac191](https://doi.org/10.1093/bib/bbac191)] [Medline: [35595537](https://pubmed.ncbi.nlm.nih.gov/35595537/)]
67. Quazi S. Artificial intelligence and machine learning in precision and genomic medicine. *Med Oncol*. Jun 15, 2022;39(8):120. [doi: [10.1007/s12032-022-01711-1](https://doi.org/10.1007/s12032-022-01711-1)] [Medline: [35704152](https://pubmed.ncbi.nlm.nih.gov/35704152/)]
68. Khan M. Bioinformatics and machine learning: analyzing genomic data for personalized medicine. *Open Science Framework*. Preprint posted online on Aug 8, 2023. [doi: [10.31219/osf.io/93584](https://doi.org/10.31219/osf.io/93584)]
69. Dara S, Dhamecherla S, Jadav SS, Babu CM, Ahsan MJ. Machine learning in drug discovery: a review. *Artif Intell Rev*. 2022;55(3):1947-1999. [doi: [10.1007/s10462-021-10058-4](https://doi.org/10.1007/s10462-021-10058-4)] [Medline: [34393317](https://pubmed.ncbi.nlm.nih.gov/34393317/)]
70. Kearney E, Wojcik A, Babu D. Artificial intelligence in genetic services delivery: utopia or apocalypse? *J Genet Couns*. Feb 2020;29(1):8-17. [doi: [10.1002/jgc4.1192](https://doi.org/10.1002/jgc4.1192)] [Medline: [31749317](https://pubmed.ncbi.nlm.nih.gov/31749317/)]
71. Benning L, Peintner A, Peintner L. Advances in and the applicability of machine learning-based screening and early detection approaches for cancer: a primer. *Cancers (Basel)*. Jan 26, 2022;14(3):623. [doi: [10.3390/cancers14030623](https://doi.org/10.3390/cancers14030623)] [Medline: [35158890](https://pubmed.ncbi.nlm.nih.gov/35158890/)]
72. Tao K, Bian Z, Zhang Q, et al. Machine learning-based genome-wide interrogation of somatic copy number aberrations in circulating tumor DNA for early detection of hepatocellular carcinoma. *EBioMedicine*. Jun 2020;56:102811. [doi: [10.1016/j.ebiom.2020.102811](https://doi.org/10.1016/j.ebiom.2020.102811)] [Medline: [32512514](https://pubmed.ncbi.nlm.nih.gov/32512514/)]
73. Mullen M, Zhang A, Lui GK, Romfh AW, Rhee JW, Wu JC. Race and genetics in congenital heart disease: application of iPSCs, omics, and machine learning technologies. *Front Cardiovasc Med*. 2021;8:635280. [doi: [10.3389/fcvm.2021.635280](https://doi.org/10.3389/fcvm.2021.635280)] [Medline: [33681306](https://pubmed.ncbi.nlm.nih.gov/33681306/)]
74. Cortés-Ciriano I, Gulhan DC, Lee JJK, Melloni GEM, Park PJ. Computational analysis of cancer genome sequencing data. *Nat Rev Genet*. May 2022;23(5):298-314. [doi: [10.1038/s41576-021-00431-y](https://doi.org/10.1038/s41576-021-00431-y)] [Medline: [34880424](https://pubmed.ncbi.nlm.nih.gov/34880424/)]

75. Dargan S, Kumar M. A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Syst Appl*. Apr 2020;143:113114. [doi: [10.1016/j.eswa.2019.113114](https://doi.org/10.1016/j.eswa.2019.113114)]
76. Uwaechia AN, Ramli DA. A comprehensive survey on ECG signals as new biometric modality for human authentication: recent advances and future challenges. *IEEE Access*. 2021;9:97760-97802. [doi: [10.1109/ACCESS.2021.3095248](https://doi.org/10.1109/ACCESS.2021.3095248)]
77. Paranjape RB, Mahovsky J, Benedicenti L, Koles' Z. The electroencephalogram as a biometric. Presented at: Canadian Conference on Electrical and Computer Engineering 2001; May 13-16, 2001; Toronto, ON, Canada. [doi: [10.1109/CCECE.2001.933649](https://doi.org/10.1109/CCECE.2001.933649)]
78. Franceschetti L, Lodetti G, Blandino A, Amadasi A, Bugelli V. Exploring the role of the human microbiome in forensic identification: opportunities and challenges. *Int J Legal Med*. Sep 2024;138(5):1891-1905. [doi: [10.1007/s00414-024-03217-z](https://doi.org/10.1007/s00414-024-03217-z)] [Medline: [38594499](https://pubmed.ncbi.nlm.nih.gov/38594499/)]
79. Sharma A, Kumar R, Varadwaj P. Smelling the disease: diagnostic potential of breath analysis. *Mol Diagn Ther*. May 2023;27(3):321-347. [doi: [10.1007/s40291-023-00640-7](https://doi.org/10.1007/s40291-023-00640-7)] [Medline: [36729362](https://pubmed.ncbi.nlm.nih.gov/36729362/)]
80. Abdulrahman SA, Alhayani B. A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Mater Today*. 2023;80:2642-2646. [doi: [10.1016/j.matpr.2021.07.005](https://doi.org/10.1016/j.matpr.2021.07.005)]
81. Kisku DR, Gupta P, Sing JK. Design and Implementation of Healthcare Biometric Systems. IGI Global; 2019. [doi: [10.4018/978-1-5225-7525-2](https://doi.org/10.4018/978-1-5225-7525-2)]
82. Mason J, Dave R, Chatterjee P, Graham-Allen I, Esterline A, Roy K. An investigation of biometric authentication in the healthcare environment. *Array*. Dec 2020;8:100042. [doi: [10.1016/j.array.2020.100042](https://doi.org/10.1016/j.array.2020.100042)]
83. Kaul SD, Murty VK, Hatzinakos D. Secure and privacy preserving biometric based user authentication with data access control system in the healthcare environment. Presented at: 2020 International Conference on Cyberworlds (CW); Sep 29 to Oct 1, 2020; Caen, France. [doi: [10.1109/CW49994.2020.00047](https://doi.org/10.1109/CW49994.2020.00047)]
84. Barka E, Al Baqari M, Kerrache CA, Herrera-Tapia J. Implementation of a biometric-based blockchain system for preserving privacy, security, and access control in healthcare records. *J Sens Actuator Netw*. 2022;11(4):85. [doi: [10.3390/jsan11040085](https://doi.org/10.3390/jsan11040085)]
85. Choi J h., Khamraev K, Cheriyan D. Hybrid health risk assessment model using real-time particulate matter, biometrics, and benchmark device. *J Clean Prod*. May 2022;350:131443. [doi: [10.1016/j.jclepro.2022.131443](https://doi.org/10.1016/j.jclepro.2022.131443)]
86. Baseri Y, Hafid A, Firoozjaei MD, Cherkaoui S, Ray I. Statistical privacy protection for secure data access control in cloud. *J Inf Secur Appl*. Aug 2024;84:103823. [doi: [10.1016/j.jisa.2024.103823](https://doi.org/10.1016/j.jisa.2024.103823)]
87. Riplinger L, Piera-Jiménez J, Dooling JP. Patient identification techniques - approaches, implications, and findings. *Yearb Med Inform*. Aug 2020;29(1):81-86. [doi: [10.1055/s-0040-1701984](https://doi.org/10.1055/s-0040-1701984)] [Medline: [32823300](https://pubmed.ncbi.nlm.nih.gov/32823300/)]
88. Sohn JW, Kim H, Park SB, et al. Clinical study of using biometrics to identify patient and procedure. *Front Oncol*. 2020;10:586232. [doi: [10.3389/fonc.2020.586232](https://doi.org/10.3389/fonc.2020.586232)] [Medline: [33335855](https://pubmed.ncbi.nlm.nih.gov/33335855/)]
89. Fatimah B, Singh P, Singhal A, Pachori RB. Biometric identification from ECG signals using Fourier decomposition and machine learning. *IEEE Trans Instrum Meas*. 2022;71:1-9. [doi: [10.1109/TIM.2022.3199260](https://doi.org/10.1109/TIM.2022.3199260)]
90. Prakash AJ, Patro KK, Samantray S, Pławiak P, Hammad M. A deep learning technique for biometric authentication using ECG beat template matching. *Information*. 2023;14(2):65. [doi: [10.3390/info14020065](https://doi.org/10.3390/info14020065)]
91. Mohsin AH, Zaidan AA, Zaidan BB, et al. Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: a multi-layer systematic review. *J Med Syst*. Oct 16, 2018;42(12):1-36. [doi: [10.1007/s10916-018-1104-5](https://doi.org/10.1007/s10916-018-1104-5)] [Medline: [30327939](https://pubmed.ncbi.nlm.nih.gov/30327939/)]
92. Ismail SNA, Nayan NA, Jaafar R, May Z. Recent advances in non-invasive blood pressure monitoring and prediction using a machine learning approach. *Sensors (Basel)*. Aug 18, 2022;22(16):6195. [doi: [10.3390/s22166195](https://doi.org/10.3390/s22166195)] [Medline: [36015956](https://pubmed.ncbi.nlm.nih.gov/36015956/)]
93. Fei C, Liu R, Li Z, Wang T, Baig FN. Machine and deep learning algorithms for wearable health monitoring. In: Manocha AK, Jain S, Singh M, Paul S, editors. *Computational Intelligence in Healthcare Health Information Science*. Springer; 2021:105-160. [doi: [10.1007/978-3-030-68723-6_6](https://doi.org/10.1007/978-3-030-68723-6_6)]
94. Gomes N, Pato M, Lourenço AR, Datia N. A survey on wearable sensors for mental health monitoring. *Sensors (Basel)*. Jan 25, 2023;23(3):1330. [doi: [10.3390/s23031330](https://doi.org/10.3390/s23031330)] [Medline: [36772370](https://pubmed.ncbi.nlm.nih.gov/36772370/)]
95. Killoran J, Cui Y (Gina), Park A, van Esch P, Kietzmann J. Can behavioral biometrics make everyone happy? *Bus Horiz*. Sep 2023;66(5):585-591. [doi: [10.1016/j.bushor.2023.02.001](https://doi.org/10.1016/j.bushor.2023.02.001)]
96. Garcia-Ceja E, Riegler M, Nordgreen T, Jakobsen P, Oedegaard KJ, Tørresen J. Mental health monitoring with multimodal sensing and machine learning: a survey. *Pervasive Mob Comput*. Dec 2018;51:1-26. [doi: [10.1016/j.pmcj.2018.09.003](https://doi.org/10.1016/j.pmcj.2018.09.003)]
97. Harrer S, Shah P, Antony B, Hu J. Artificial intelligence for clinical trial design. *Trends Pharmacol Sci*. Aug 2019;40(8):577-591. [doi: [10.1016/j.tips.2019.05.005](https://doi.org/10.1016/j.tips.2019.05.005)] [Medline: [31326235](https://pubmed.ncbi.nlm.nih.gov/31326235/)]

98. Weessler EH, Naumann T, Andersson T, et al. The role of machine learning in clinical research: transforming the future of evidence generation. *Trials*. Aug 16, 2021;22(1):537. [doi: [10.1186/s13063-021-05489-x](https://doi.org/10.1186/s13063-021-05489-x)] [Medline: [34399832](https://pubmed.ncbi.nlm.nih.gov/34399832/)]
99. Moro-Velazquez L, Gomez-Garcia JA, Arias-Londoño JD, Dehak N, Godino-Llorente JI. Advances in Parkinson's disease detection and assessment using voice and speech: a review of the articulatory and phonatory aspects. *Biomed Signal Process Control*. Apr 2021;66:102418. [doi: [10.1016/j.bspc.2021.102418](https://doi.org/10.1016/j.bspc.2021.102418)]
100. Ngo QC, Motin MA, Pah ND, Drotár P, Kempster P, Kumar D. Computerized analysis of speech and voice for Parkinson's disease: a systematic review. *Comput Methods Programs Biomed*. Nov 2022;226:107133. [doi: [10.1016/j.cmpb.2022.107133](https://doi.org/10.1016/j.cmpb.2022.107133)] [Medline: [36183641](https://pubmed.ncbi.nlm.nih.gov/36183641/)]
101. Lella KK, Pja A. Automatic COVID-19 disease diagnosis using 1D convolutional neural network and augmentation with human respiratory sound based on parameters: cough, breath, and voice. *AIMS Public Health*. 2021;8(2):240-264. [doi: [10.3934/publichealth.2021019](https://doi.org/10.3934/publichealth.2021019)] [Medline: [34017889](https://pubmed.ncbi.nlm.nih.gov/34017889/)]
102. Idrisoglu A, Dallora AL, Anderberg P, Berglund JS. Applied machine learning techniques to diagnose voice-affecting conditions and disorders: systematic literature review. *J Med Internet Res*. Jul 19, 2023;25:e46105. [doi: [10.2196/46105](https://doi.org/10.2196/46105)] [Medline: [37467031](https://pubmed.ncbi.nlm.nih.gov/37467031/)]
103. Lyakso E, Frolova O, Nikolaev A. Voice and speech features as a diagnostic symptom. In: *Psychological Applications and Trends*. 2021:359-363. URL: <https://inpact-psychologyconference.org/wp-content/uploads/2021/05/2021inpact074.pdf> [Accessed 2026-05-07] [doi: [10.36315/2021inpact074](https://doi.org/10.36315/2021inpact074)]
104. Onyema EM, Shukla PK, Dalal S, Mathur MN, Zakariah M, Tiwari B. Enhancement of patient facial recognition through deep learning algorithm: ConvNet. *J Healthc Eng*. 2021;2021:5196000. [doi: [10.1155/2021/5196000](https://doi.org/10.1155/2021/5196000)] [Medline: [34912534](https://pubmed.ncbi.nlm.nih.gov/34912534/)]
105. Jeon B, Jeong B, Jee S, et al. A facial recognition mobile app for patient safety and biometric identification: design, development, and validation. *JMIR Mhealth Uhealth*. Apr 8, 2019;7(4):e11472. [doi: [10.2196/11472](https://doi.org/10.2196/11472)] [Medline: [30958275](https://pubmed.ncbi.nlm.nih.gov/30958275/)]
106. Ghazal TM, Hasan MK, Alshurideh MT, et al. IoT for smart cities: machine learning approaches in smart healthcare—a review. *Future Internet*. 2021;13(8):218. [doi: [10.3390/fi13080218](https://doi.org/10.3390/fi13080218)]
107. Balakrishna S, Thirumaran M, Solanki VK. Iot sensor data integration in healthcare using semantics and machine learning approaches. In: Balas V, Solanki V, Kumar R, Ahad M, editors. *A Handbook of Internet of Things in Biomedical and Cyber Physical System Intelligent Systems Reference Library*. Springer; 2020:275-300. [doi: [10.1007/978-3-030-23983-1_11](https://doi.org/10.1007/978-3-030-23983-1_11)]
108. Lv Z, Li Y. Wearable sensors for vital signs measurement: a survey. *J Sens Actuator Netw*. 2022;11(1):19. [doi: [10.3390/jsan11010019](https://doi.org/10.3390/jsan11010019)]
109. Junaid SB, Imam AA, Shuaibu AN, et al. Artificial intelligence, sensors and vital health signs: a review. *Appl Sci (Basel)*. 2022;12(22):11475. [doi: [10.3390/app122211475](https://doi.org/10.3390/app122211475)]
110. Gupta N, Gupta SK, Pathak RK, Jain V, Rashidi P, Suri JS. Human activity recognition in artificial intelligence framework: a narrative review. *Artif Intell Rev*. 2022;55(6):4755-4808. [doi: [10.1007/s10462-021-10116-x](https://doi.org/10.1007/s10462-021-10116-x)] [Medline: [35068651](https://pubmed.ncbi.nlm.nih.gov/35068651/)]
111. Zhu T, Uduku C, Li K, Herrero P, Oliver N, Georgiou P. Enhancing self-management in type 1 diabetes with wearables and deep learning. *NPJ Digit Med*. Jun 27, 2022;5(1):78. [doi: [10.1038/s41746-022-00626-5](https://doi.org/10.1038/s41746-022-00626-5)] [Medline: [35760819](https://pubmed.ncbi.nlm.nih.gov/35760819/)]
112. Liyakat KKS. Heart health monitoring using IoT and machine learning methods. In: Shaik A, editor. *AI-Powered Advances in Pharmacology*. IGI Global; 2025:257-282. [doi: [10.4018/979-8-3693-3212-2.ch010](https://doi.org/10.4018/979-8-3693-3212-2.ch010)]
113. Kwon SH, Dong L. Flexible sensors and machine learning for heart monitoring. *Nano Energy*. Nov 2022;102:107632. [doi: [10.1016/j.nanoen.2022.107632](https://doi.org/10.1016/j.nanoen.2022.107632)]
114. Lin SY, Tsai CY, Majumdar A, et al. Combining a wireless radar sleep monitoring device with deep machine learning techniques to assess obstructive sleep apnea severity. *J Clin Sleep Med*. Aug 1, 2024;20(8):1267-1277. [doi: [10.5664/jcsm.11136](https://doi.org/10.5664/jcsm.11136)] [Medline: [38546033](https://pubmed.ncbi.nlm.nih.gov/38546033/)]
115. Arora A, Chakraborty P, Bhatia MPS. Analysis of data from wearable sensors for sleep quality estimation and prediction using deep learning. *Arab J Sci Eng*. Dec 2020;45(12):10793-10812. [doi: [10.1007/s13369-020-04877-w](https://doi.org/10.1007/s13369-020-04877-w)]
116. Zhang W, Ram S. A comprehensive analysis of triggers and risk factors for asthma based on machine learning and large heterogeneous data sources. *MIS Q*. Mar 1, 2020;44(1):305-350. [doi: [10.25300/MISQ/2020/15106](https://doi.org/10.25300/MISQ/2020/15106)]
117. Bohlmann A, Mostafa J, Kumar M. Machine learning and medication adherence: scoping review. *JMIRx Med*. Nov 24, 2021;2(4):e26993. [doi: [10.2196/26993](https://doi.org/10.2196/26993)] [Medline: [37725549](https://pubmed.ncbi.nlm.nih.gov/37725549/)]
118. Roh H, Shin S, Han J, Lim S. A deep learning-based medication behavior monitoring system. *Math Biosci Eng*. Jan 28, 2021;18(2):1513-1528. [doi: [10.3934/mbe.2021078](https://doi.org/10.3934/mbe.2021078)] [Medline: [33757196](https://pubmed.ncbi.nlm.nih.gov/33757196/)]
119. Meyer BM, Tulipani LJ, Gurchiek RD, et al. Wearables and deep learning classify fall risk from gait in multiple sclerosis. *IEEE J Biomed Health Inform*. 2020;25(5):1824-1831. [doi: [10.1109/JBHI.2020.3025049](https://doi.org/10.1109/JBHI.2020.3025049)]
120. Kyamakya K, Al-Machot F, Haj Mosa A, Bouchachia H, Chedjou JC, Bagula A. Emotion and stress recognition related sensors and machine learning technologies. *Sensors (Basel)*. Mar 24, 2021;21(7):2273. [doi: [10.3390/s21072273](https://doi.org/10.3390/s21072273)] [Medline: [33804987](https://pubmed.ncbi.nlm.nih.gov/33804987/)]

121. Gedam S, Paul S. A review on mental stress detection using wearable sensors and machine learning techniques. *IEEE Access*. 2021;9:84045-84066. [doi: [10.1109/ACCESS.2021.3085502](https://doi.org/10.1109/ACCESS.2021.3085502)]
122. Fountzilias E, Pearce T, Baysal MA, Chakraborty A, Tsimberidou AM. Convergence of evolving artificial intelligence and machine learning techniques in precision oncology. *NPJ Digit Med*. Jan 31, 2025;8(1):75. [doi: [10.1038/s41746-025-01471-y](https://doi.org/10.1038/s41746-025-01471-y)] [Medline: [39890986](https://pubmed.ncbi.nlm.nih.gov/39890986/)]
123. Acosta JN, Falcone GJ, Rajpurkar P, Topol EJ. Multimodal biomedical AI. *Nat Med*. Sep 2022;28(9):1773-1784. [doi: [10.1038/s41591-022-01981-2](https://doi.org/10.1038/s41591-022-01981-2)] [Medline: [36109635](https://pubmed.ncbi.nlm.nih.gov/36109635/)]
124. Hsueh PYS, Dey S, Das S, Wetter T. Making sense of patient-generated health data for interpretable patient-centered care: the transition from “more” to “better.” In: Gundlapalli AV, Jaulent MC, Zhao D, editors. *MEDINFO 2017: Precision Healthcare through Informatics*. IOS Press; 2017:113-117. [doi: [10.3233/978-1-61499-830-3-113](https://doi.org/10.3233/978-1-61499-830-3-113)]
125. Mendo IR, Marques G, de la Torre Díez I, López-Coronado M, Martín-Rodríguez F. Machine learning in medical emergencies: a systematic review and analysis. *J Med Syst*. Aug 18, 2021;45(10):88. [doi: [10.1007/s10916-021-01762-3](https://doi.org/10.1007/s10916-021-01762-3)] [Medline: [34410512](https://pubmed.ncbi.nlm.nih.gov/34410512/)]
126. van der Boon RMA, Camm AJ, Aguiar C, et al. Risks and benefits of sharing patient information on social media: a digital dilemma. *Eur Heart J Digit Health*. May 2024;5(3):199-207. [doi: [10.1093/ehjdh/ztae009](https://doi.org/10.1093/ehjdh/ztae009)] [Medline: [38774369](https://pubmed.ncbi.nlm.nih.gov/38774369/)]
127. Gupta A, Katarya R. Social media based surveillance systems for healthcare using machine learning: a systematic review. *J Biomed Inform*. Aug 2020;108:103500. [doi: [10.1016/j.jbi.2020.103500](https://doi.org/10.1016/j.jbi.2020.103500)] [Medline: [32622833](https://pubmed.ncbi.nlm.nih.gov/32622833/)]
128. Hasib KM, Islam MR, Sakib S, Akbar MA, Razzak I, Alam MS. Depression detection from social networks data based on machine learning and deep learning techniques: an interrogative survey. *IEEE Trans Comput Soc Syst*. 2023;10(4):1568-1586. [doi: [10.1109/TCSS.2023.3263128](https://doi.org/10.1109/TCSS.2023.3263128)]
129. Johnson KB, Wei WQ, Weeraratne D, et al. Precision medicine, AI, and the future of personalized health care. *Clin Transl Sci*. Jan 2021;14(1):86-93. [doi: [10.1111/cts.12884](https://doi.org/10.1111/cts.12884)] [Medline: [32961010](https://pubmed.ncbi.nlm.nih.gov/32961010/)]
130. Verma S, Malviya R, Alam MA, Tripathi BD. Tele-health monitoring using artificial intelligence deep learning framework. In: Malviya R, Ghinea G, Dhanaraj RK, Balusamy B, Sundram S, editors. *Deep Learning for Targeted Treatments: Transformation in Healthcare*. Scrivener Publishing; 2022:199-228. [doi: [10.1002/9781119857983](https://doi.org/10.1002/9781119857983)]
131. Moorthy V, Abubakar I, Qadri F, et al. The future of the global clinical trial ecosystem: a vision from the first WHO Global Clinical Trials Forum. *The Lancet*. Jan 2024;403(10422):124-126. [doi: [10.1016/S0140-6736\(23\)02798-8](https://doi.org/10.1016/S0140-6736(23)02798-8)]
132. Pettit RW, Fullem R, Cheng C, Amos CI. Artificial intelligence, machine learning, and deep learning for clinical outcome prediction. *Emerg Top Life Sci*. Dec 20, 2021;5(6):729-745. [doi: [10.1042/ETLS20210246](https://doi.org/10.1042/ETLS20210246)] [Medline: [34927670](https://pubmed.ncbi.nlm.nih.gov/34927670/)]
133. Cohen IG. Informed consent and medical artificial intelligence: what to tell the patient? *SSRN Journal*. 2019;108. [doi: [10.2139/ssrn.3529576](https://doi.org/10.2139/ssrn.3529576)]
134. McKeown A, Mourby M, Harrison P, Walker S, Sheehan M, Singh I. Ethical issues in consent for the reuse of data in health data platforms. *Sci Eng Ethics*. Feb 4, 2021;27(1):9. [doi: [10.1007/s11948-021-00282-0](https://doi.org/10.1007/s11948-021-00282-0)] [Medline: [33538942](https://pubmed.ncbi.nlm.nih.gov/33538942/)]
135. Chien I, Enrique A, Palacios J, et al. A machine learning approach to understanding patterns of engagement with internet-delivered mental health interventions. *JAMA Netw Open*. Jul 1, 2020;3(7):e2010791. [doi: [10.1001/jamanetworkopen.2020.10791](https://doi.org/10.1001/jamanetworkopen.2020.10791)] [Medline: [32678450](https://pubmed.ncbi.nlm.nih.gov/32678450/)]
136. Benke K, Benke G. Artificial intelligence and big data in public health. *Int J Environ Res Public Health*. Dec 10, 2018;15(12):2796. [doi: [10.3390/ijerph15122796](https://doi.org/10.3390/ijerph15122796)] [Medline: [30544648](https://pubmed.ncbi.nlm.nih.gov/30544648/)]
137. Song L, Li Y, Nie S, et al. Using machine learning to predict adverse events in acute coronary syndrome: a retrospective study. *Clin Cardiol*. Dec 2023;46(12):1594-1602. [doi: [10.1002/clc.24127](https://doi.org/10.1002/clc.24127)] [Medline: [37654030](https://pubmed.ncbi.nlm.nih.gov/37654030/)]
138. Yang J, Wan J, Feng L, et al. Machine learning algorithms for the prediction of adverse prognosis in patients undergoing peritoneal dialysis. *BMC Med Inform Decis Mak*. Jan 2, 2024;24(1):8. [doi: [10.1186/s12911-023-02412-z](https://doi.org/10.1186/s12911-023-02412-z)] [Medline: [38166909](https://pubmed.ncbi.nlm.nih.gov/38166909/)]
139. Badwan BA, Liaropoulos G, Kyrodimos E, Skaltsas D, Tsirigos A, Gorgoulis VG. Machine learning approaches to predict drug efficacy and toxicity in oncology. *Cell Rep Methods*. Feb 27, 2023;3(2):100413. [doi: [10.1016/j.crmeth.2023.100413](https://doi.org/10.1016/j.crmeth.2023.100413)] [Medline: [36936080](https://pubmed.ncbi.nlm.nih.gov/36936080/)]
140. Feijoo F, Palopoli M, Bernstein J, Siddiqui S, Albright TE. Key indicators of phase transition for clinical trials through machine learning. *Drug Discov Today*. Feb 2020;25(2):414-421. [doi: [10.1016/j.drudis.2019.12.014](https://doi.org/10.1016/j.drudis.2019.12.014)] [Medline: [31926317](https://pubmed.ncbi.nlm.nih.gov/31926317/)]
141. MacEachern SJ, Forkert ND. Machine learning for precision medicine. *Genome*. Apr 2021;64(4):416-425. [doi: [10.1139/gen-2020-0131](https://doi.org/10.1139/gen-2020-0131)] [Medline: [33091314](https://pubmed.ncbi.nlm.nih.gov/33091314/)]
142. Chalasani SH, Syed J, Ramesh M, Patil V, Pramod Kumar TM. Artificial intelligence in the field of pharmacy practice: a literature review. *Explor Res Clin Soc Pharm*. Dec 2023;12:100346. [doi: [10.1016/j.rcsop.2023.100346](https://doi.org/10.1016/j.rcsop.2023.100346)] [Medline: [37885437](https://pubmed.ncbi.nlm.nih.gov/37885437/)]
143. Askr H, Elgeldawi E, Aboul Ella H, Elshaier Y, Gomaa MM, Hassanien AE. Deep learning in drug discovery: an integrative review and future challenges. *Artif Intell Rev*. 2023;56(7):5975-6037. [doi: [10.1007/s10462-022-10306-1](https://doi.org/10.1007/s10462-022-10306-1)] [Medline: [36415536](https://pubmed.ncbi.nlm.nih.gov/36415536/)]

144. Li Q, Tang B, Wu Y, et al. Machine learning: a new approach for dose individualization. *Clin Pharma and Therapeutics*. Apr 2024;115(4):727-744. [doi: [10.1002/cpt.3049](https://doi.org/10.1002/cpt.3049)]
145. Del Fabro L, Bondi E, Serio F, Maggioni E, D'Agostino A, Brambilla P. Machine learning methods to predict outcomes of pharmacological treatment in psychosis. *Transl Psychiatry*. Mar 2, 2023;13(1):75. [doi: [10.1038/s41398-023-02371-z](https://doi.org/10.1038/s41398-023-02371-z)] [Medline: [36864017](https://pubmed.ncbi.nlm.nih.gov/36864017/)]
146. D'Costa A, Zatale A. AI and the cardiologist: when mind, heart and machine unite. *Open Heart*. Dec 2021;8(2):e001874. [doi: [10.1136/openhrt-2021-001874](https://doi.org/10.1136/openhrt-2021-001874)] [Medline: [34949649](https://pubmed.ncbi.nlm.nih.gov/34949649/)]
147. Hasan MM, Young GJ, Shi J, et al. A machine learning based two-stage clinical decision support system for predicting patients' discontinuation from opioid use disorder treatment: retrospective observational study. *BMC Med Inform Decis Mak*. Nov 26, 2021;21(1):331. [doi: [10.1186/s12911-021-01692-7](https://doi.org/10.1186/s12911-021-01692-7)] [Medline: [34836524](https://pubmed.ncbi.nlm.nih.gov/34836524/)]
148. Kim HR, Sung M, Park JA, et al. Analyzing adverse drug reaction using statistical and machine learning methods: a systematic review. *Medicine (Baltimore)*. Jun 24, 2022;101(25):e29387. [doi: [10.1097/MD.00000000000029387](https://doi.org/10.1097/MD.00000000000029387)] [Medline: [35758373](https://pubmed.ncbi.nlm.nih.gov/35758373/)]
149. Zhang S, Bamakan SMH, Qu Q, Li S. Learning for personalized medicine: a comprehensive review from a deep learning perspective. *IEEE Rev Biomed Eng*. 2019;12:194-208. [doi: [10.1109/RBME.2018.2864254](https://doi.org/10.1109/RBME.2018.2864254)] [Medline: [30106692](https://pubmed.ncbi.nlm.nih.gov/30106692/)]
150. Meng W, Zhang X, Ru B, Guan Y. A machine learning approach to real-world time to treatment discontinuation prediction. *Advanced Intelligent Systems*. Apr 2023;5(4):2200254. URL: <https://advanced.onlinelibrary.wiley.com/doi/10.1002/aisy.202200254> [doi: [10.1002/aisy.202200254](https://doi.org/10.1002/aisy.202200254)]
151. Gu Y, Zalkikar A, Liu M, et al. Predicting medication adherence using ensemble learning and deep learning models with large scale healthcare data. *Sci Rep*. Sep 23, 2021;11(1):18961. [doi: [10.1038/s41598-021-98387-w](https://doi.org/10.1038/s41598-021-98387-w)] [Medline: [34556746](https://pubmed.ncbi.nlm.nih.gov/34556746/)]
152. Khan S, Sajjad M, Hussain T, Ullah A, Imran AS. A review on traditional machine learning and deep learning models for WBCs classification in blood smear images. *IEEE Access*. 2020;9:10657-10673. [doi: [10.1109/ACCESS.2020.3048172](https://doi.org/10.1109/ACCESS.2020.3048172)]
153. De Bruyne S, De Kesel P, Oyaert M. Applications of artificial intelligence in urinalysis: is the future already here? *Clin Chem*. Dec 1, 2023;69(12):1348-1360. [doi: [10.1093/clinchem/hvad136](https://doi.org/10.1093/clinchem/hvad136)] [Medline: [37708293](https://pubmed.ncbi.nlm.nih.gov/37708293/)]
154. Goodswen SJ, Barratt JLN, Kennedy PJ, Kaufer A, Calarco L, Ellis JT. Machine learning and applications in microbiology. *FEMS Microbiol Rev*. Sep 8, 2021;45(5):fuab015. [doi: [10.1093/femsre/fuab015](https://doi.org/10.1093/femsre/fuab015)] [Medline: [33724378](https://pubmed.ncbi.nlm.nih.gov/33724378/)]
155. Ghannam RB, Techtmann SM. Machine learning applications in microbial ecology, human microbiome studies, and environmental monitoring. *Comput Struct Biotechnol J*. 2021;19:1092-1107. [doi: [10.1016/j.csbj.2021.01.028](https://doi.org/10.1016/j.csbj.2021.01.028)] [Medline: [33680353](https://pubmed.ncbi.nlm.nih.gov/33680353/)]
156. Unger M, Kather JN. Deep learning in cancer genomics and histopathology. *Genome Med*. Mar 27, 2024;16(1):44. [doi: [10.1186/s13073-024-01315-6](https://doi.org/10.1186/s13073-024-01315-6)] [Medline: [38539231](https://pubmed.ncbi.nlm.nih.gov/38539231/)]
157. Obstfeld AE. Hematology and machine learning. *J Appl Lab Med*. Jan 4, 2023;8(1):129-144. [doi: [10.1093/jalm/jfac108](https://doi.org/10.1093/jalm/jfac108)] [Medline: [36610431](https://pubmed.ncbi.nlm.nih.gov/36610431/)]
158. Danieli MG, Brunetto S, Gammari L, et al. Machine learning application in autoimmune diseases: state of art and future prospectives. *Autoimmun Rev*. Feb 2024;23(2):103496. [doi: [10.1016/j.autrev.2023.103496](https://doi.org/10.1016/j.autrev.2023.103496)] [Medline: [38081493](https://pubmed.ncbi.nlm.nih.gov/38081493/)]
159. Usategui I, Barbado J, Torres AM, Cascón J, Mateo J. Machine learning, a new tool for the detection of immunodeficiency patterns in systemic lupus erythematosus. *J Investig Med*. Oct 2023;71(7):742-752. [doi: [10.1177/10815589231171404](https://doi.org/10.1177/10815589231171404)] [Medline: [37158077](https://pubmed.ncbi.nlm.nih.gov/37158077/)]
160. Thomasian NM, Kamel IR, Bai HX. Machine intelligence in non-invasive endocrine cancer diagnostics. *Nat Rev Endocrinol*. Feb 2022;18(2):81-95. [doi: [10.1038/s41574-021-00543-9](https://doi.org/10.1038/s41574-021-00543-9)] [Medline: [34754064](https://pubmed.ncbi.nlm.nih.gov/34754064/)]
161. Hong N, Park H, Rhee Y. Machine learning applications in endocrinology and metabolism research: an overview. *Endocrinol Metab*. Mar 2020;35(1):71-84. [doi: [10.3803/EnM.2020.35.1.71](https://doi.org/10.3803/EnM.2020.35.1.71)]
162. Amjad A, Kordel P, Fernandes G. A review on innovation in healthcare sector (telehealth) through artificial intelligence. *Sustainability*. 2023;15(8):6655. [doi: [10.3390/su15086655](https://doi.org/10.3390/su15086655)]
163. Gajarawala SN, Pelkowski JN. Telehealth benefits and barriers. *J Nurse Pract*. Feb 2021;17(2):218-221. [doi: [10.1016/j.nurpra.2020.09.013](https://doi.org/10.1016/j.nurpra.2020.09.013)] [Medline: [33106751](https://pubmed.ncbi.nlm.nih.gov/33106751/)]
164. Schünke LC, Mello B, da Costa CA, et al. A rapid review of machine learning approaches for telemedicine in the scope of COVID-19. *Artif Intell Med*. Jul 2022;129:102312. [doi: [10.1016/j.artmed.2022.102312](https://doi.org/10.1016/j.artmed.2022.102312)] [Medline: [35659388](https://pubmed.ncbi.nlm.nih.gov/35659388/)]
165. Hou Y, Huang J. Natural language processing for social science research: a comprehensive review. *Chin J Sociol*. Jan 2025;11(1):121-157. [doi: [10.1177/2057150X241306780](https://doi.org/10.1177/2057150X241306780)]
166. Hughes A, Shandhi MMH, Master H, Dunn J, Brittain E. Wearable devices in cardiovascular medicine. *Circ Res*. Mar 3, 2023;132(5):652-670. [doi: [10.1161/CIRCRESAHA.122.322389](https://doi.org/10.1161/CIRCRESAHA.122.322389)] [Medline: [36862812](https://pubmed.ncbi.nlm.nih.gov/36862812/)]
167. Liu Y, Wang B. Advanced applications in chronic disease monitoring using IoT mobile sensing device data, machine learning algorithms and frame theory: a systematic review. *Front Public Health*. 2025;13:1510456. [doi: [10.3389/fpubh.2025.1510456](https://doi.org/10.3389/fpubh.2025.1510456)]

168. Segal G, Segev A, Brom A, Lifshitz Y, Wasserstrum Y, Zimlichman E. Reducing drug prescription errors and adverse drug events by application of a probabilistic, machine-learning based clinical decision support system in an inpatient setting. *J Am Med Inform Assoc*. Dec 1, 2019;26(12):1560-1565. [doi: [10.1093/jamia/ocz135](https://doi.org/10.1093/jamia/ocz135)] [Medline: [31390471](https://pubmed.ncbi.nlm.nih.gov/31390471/)]
169. Verma D, Bach K, Mork PJ. Application of machine learning methods on patient reported outcome measurements for predicting outcomes: a literature review. *Informatics (MDPI)*. 2021;8(3):56. [doi: [10.3390/informatics8030056](https://doi.org/10.3390/informatics8030056)]
170. Björneld O, Carlsson M, Löwe W. Case study - Feature engineering inspired by domain experts on real world medical data. *Intelligence-Based Medicine*. 2023;8:100110. [doi: [10.1016/j.ibmed.2023.100110](https://doi.org/10.1016/j.ibmed.2023.100110)]
171. Xu X, Li J, Zhu Z, et al. A comprehensive review on synergy of multi-modal data and AI technologies in medical diagnosis. *Bioengineering (Basel)*. Feb 25, 2024;11(3):219. [doi: [10.3390/bioengineering11030219](https://doi.org/10.3390/bioengineering11030219)] [Medline: [38534493](https://pubmed.ncbi.nlm.nih.gov/38534493/)]
172. Zhou SK, Greenspan H, Davatzikos C, et al. A review of deep learning in medical imaging: imaging traits, technology trends, case studies with progress highlights, and future promises. *Proc IEEE*. 2021;109(5):820-838. [doi: [10.1109/JPROC.2021.3054390](https://doi.org/10.1109/JPROC.2021.3054390)]
173. Khalifa M, Albadaawy M. AI in diagnostic imaging: revolutionising accuracy and efficiency. *Computer Methods and Programs in Biomedicine Update*. 2024;5:100146. URL: <https://www.sciencedirect.com/science/article/pii/S2666990024000132> [Accessed 2026-06-01]
174. Aggarwal R, Sounderajah V, Martin G, et al. Diagnostic accuracy of deep learning in medical imaging: a systematic review and meta-analysis. *NPJ Digit Med*. Apr 7, 2021;4(1):65. [doi: [10.1038/s41746-021-00438-z](https://doi.org/10.1038/s41746-021-00438-z)] [Medline: [33828217](https://pubmed.ncbi.nlm.nih.gov/33828217/)]
175. Prasad VK, Verma A, Bhattacharya P, et al. Revolutionizing healthcare: a comparative insight into deep learning's role in medical imaging. *Sci Rep*. Dec 4, 2024;14(1):30273. [doi: [10.1038/s41598-024-71358-7](https://doi.org/10.1038/s41598-024-71358-7)] [Medline: [39632902](https://pubmed.ncbi.nlm.nih.gov/39632902/)]
176. Zhang K, Yang X, Wang Y, et al. Artificial intelligence in drug development. *Nat Med*. Jan 2025;31(1):45-59. [doi: [10.1038/s41591-024-03434-4](https://doi.org/10.1038/s41591-024-03434-4)] [Medline: [39833407](https://pubmed.ncbi.nlm.nih.gov/39833407/)]
177. Kant S, Roy S. Artificial intelligence in drug discovery and development: transforming challenges into opportunities. *Discov Pharm Sci*. 2025;1(1):7. [doi: [10.1007/s44395-025-00007-3](https://doi.org/10.1007/s44395-025-00007-3)]
178. Gomes B, Ashley EA. Artificial intelligence in molecular medicine. *N Engl J Med*. Jun 29, 2023;388(26):2456-2465. [doi: [10.1056/NEJMr2204787](https://doi.org/10.1056/NEJMr2204787)] [Medline: [37379136](https://pubmed.ncbi.nlm.nih.gov/37379136/)]
179. Davis S, Zhang J, Lee I, et al. Effective hospital readmission prediction models using machine-learned features. *BMC Health Serv Res*. Nov 24, 2022;22(1):1415. [doi: [10.1186/s12913-022-08748-y](https://doi.org/10.1186/s12913-022-08748-y)] [Medline: [36434628](https://pubmed.ncbi.nlm.nih.gov/36434628/)]
180. Dixon D, Sattar H, Moros N, et al. Unveiling the influence of AI predictive analytics on patient outcomes: a comprehensive narrative review. *Cureus*. May 2024;16(5):e59954. [doi: [10.7759/cureus.59954](https://doi.org/10.7759/cureus.59954)] [Medline: [38854327](https://pubmed.ncbi.nlm.nih.gov/38854327/)]
181. Oh EG, Oh S, Cho S, Moon M. Predicting readmission among high-risk discharged patients using a machine learning model with nursing data: retrospective study. *JMIR Med Inform*. Mar 5, 2025;13:e56671. [doi: [10.2196/56671](https://doi.org/10.2196/56671)] [Medline: [40106364](https://pubmed.ncbi.nlm.nih.gov/40106364/)]
182. Varghese C, Harrison EM, O'Grady G, Topol EJ. Artificial intelligence in surgery. *Nat Med*. May 2024;30(5):1257-1268. [doi: [10.1038/s41591-024-02970-3](https://doi.org/10.1038/s41591-024-02970-3)] [Medline: [38740998](https://pubmed.ncbi.nlm.nih.gov/38740998/)]
183. Antel R, Abbasgholizadeh-Rahimi S, Guadagno E, Harley JM, Poenaru D. The use of artificial intelligence and virtual reality in doctor-patient risk communication: a scoping review. *Patient Educ Couns*. Oct 2022;105(10):3038-3050. [doi: [10.1016/j.pec.2022.06.006](https://doi.org/10.1016/j.pec.2022.06.006)] [Medline: [35725526](https://pubmed.ncbi.nlm.nih.gov/35725526/)]
184. Wah JNK. Revolutionizing e-health: the transformative role of AI-powered hybrid chatbots in healthcare solutions. *Front Public Health*. 2025;13:1530799. [doi: [10.3389/fpubh.2025.1530799](https://doi.org/10.3389/fpubh.2025.1530799)] [Medline: [40017541](https://pubmed.ncbi.nlm.nih.gov/40017541/)]
185. Alowais SA, Alghamdi SS, Alsuhebany N, et al. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. *BMC Med Educ*. Sep 22, 2023;23(1):689. [doi: [10.1186/s12909-023-04698-z](https://doi.org/10.1186/s12909-023-04698-z)] [Medline: [37740191](https://pubmed.ncbi.nlm.nih.gov/37740191/)]
186. Davenport T, Kalakota R. The potential for artificial intelligence in healthcare. *Future Healthc J*. Jun 2019;6(2):94-98. [doi: [10.7861/futurehosp.6-2-94](https://doi.org/10.7861/futurehosp.6-2-94)] [Medline: [31363513](https://pubmed.ncbi.nlm.nih.gov/31363513/)]
187. Bravo F, Braun M, Farias V, et al. Optimization-driven framework to understand health care network costs and resource allocation. *Health Care Manag Sci*. Sep 2021;24(3):640-660. [doi: [10.1007/s10729-021-09565-1](https://doi.org/10.1007/s10729-021-09565-1)] [Medline: [33942227](https://pubmed.ncbi.nlm.nih.gov/33942227/)]
188. Wong F, de la Fuente-Nunez C, Collins JJ. Leveraging artificial intelligence in the fight against infectious diseases. *Science*. Jul 14, 2023;381(6654):164-170. [doi: [10.1126/science.adh1114](https://doi.org/10.1126/science.adh1114)] [Medline: [37440620](https://pubmed.ncbi.nlm.nih.gov/37440620/)]
189. Alimadadi A, Aryal S, Manandhar I, Munroe PB, Joe B, Cheng X. Artificial intelligence and machine learning to fight COVID-19. *Physiol Genomics*. Apr 1, 2020;52(4):200-202. [doi: [10.1152/physiolgenomics.00029.2020](https://doi.org/10.1152/physiolgenomics.00029.2020)] [Medline: [32216577](https://pubmed.ncbi.nlm.nih.gov/32216577/)]
190. Bhardhwaj HS, Tutika S, Kaushik L.S. S, Gupta PK, Reddy K.S. T. Artificial intelligence in vaccine development. In: Zarrintaj P, Yazdi MK, Bencherif SA, Saeb MR, Mozafari M, editors. *Artificial Intelligence in Biomaterials Design and Development*. Woodhead Publishing; 2026:185-223. [doi: [10.1016/B978-0-323-95464-8.00012-8](https://doi.org/10.1016/B978-0-323-95464-8.00012-8)]
191. Wang L, Zhang Y, Wang D, et al. Artificial intelligence for COVID-19: a systematic review. *Front Med*. 2021;8:704256. [doi: [10.3389/fmed.2021.704256](https://doi.org/10.3389/fmed.2021.704256)]
192. Lo Vercio L, Amador K, Bannister JJ, et al. Supervised machine learning tools: a tutorial for clinicians. *J Neural Eng*. Nov 19, 2020;17(6):062001. [doi: [10.1088/1741-2552/abbff2](https://doi.org/10.1088/1741-2552/abbff2)] [Medline: [33036008](https://pubmed.ncbi.nlm.nih.gov/33036008/)]

216. Rashidi HH, Albahra S, Robertson S, Tran NK, Hu B. Common statistical concepts in the supervised machine learning arena. *Front Oncol*. 2023;13:1130229. [doi: [10.3389/fonc.2023.1130229](https://doi.org/10.3389/fonc.2023.1130229)] [Medline: [36845729](https://pubmed.ncbi.nlm.nih.gov/36845729/)]
217. Esteva A, Kuprel B, Novoa RA, et al. Dermatologist-level classification of skin cancer with deep neural networks. *Nature New Biol*. Feb 2, 2017;542(7639):115-118. [doi: [10.1038/nature21056](https://doi.org/10.1038/nature21056)]
218. Shah D, Patel S, Bharti SK. Heart disease prediction using machine learning techniques. *SN Comput Sci*. Nov 2020;1(6):1-6. [doi: [10.1007/s42979-020-00365-y](https://doi.org/10.1007/s42979-020-00365-y)]
219. Levin S, Toerper M, Hamrock E, et al. Machine-learning-based electronic triage more accurately differentiates patients with respect to clinical outcomes compared with the emergency severity index. *Ann Emerg Med*. May 2018;71(5):565-574. [doi: [10.1016/j.annemergmed.2017.08.005](https://doi.org/10.1016/j.annemergmed.2017.08.005)] [Medline: [28888332](https://pubmed.ncbi.nlm.nih.gov/28888332/)]
220. Zou Q, Qu K, Luo Y, Yin D, Ju Y, Tang H. Predicting diabetes mellitus with machine learning techniques. *Front Genet*. 2018;9:515. [doi: [10.3389/fgene.2018.00515](https://doi.org/10.3389/fgene.2018.00515)] [Medline: [30459809](https://pubmed.ncbi.nlm.nih.gov/30459809/)]
221. Mucaki EJ, Zhao JZL, Lizotte DJ, Rogan PK. Predicting responses to platin chemotherapy agents with biochemically-inspired machine learning. *Signal Transduct Target Ther*. 2019;4(1):1. [doi: [10.1038/s41392-018-0034-5](https://doi.org/10.1038/s41392-018-0034-5)] [Medline: [30652029](https://pubmed.ncbi.nlm.nih.gov/30652029/)]
222. Battineni G, Sagaro GG, Chinatalapudi N, Amenta F. Applications of machine learning predictive models in the chronic disease diagnosis. *J Pers Med*. Mar 31, 2020;10(2):21. [doi: [10.3390/jpm1002021](https://doi.org/10.3390/jpm1002021)] [Medline: [32244292](https://pubmed.ncbi.nlm.nih.gov/32244292/)]
223. Dhiman P, Ma J, Andaur Navarro CL, et al. Methodological conduct of prognostic prediction models developed using machine learning in oncology: a systematic review. *BMC Med Res Methodol*. Apr 8, 2022;22(1):101. [doi: [10.1186/s12874-022-01577-x](https://doi.org/10.1186/s12874-022-01577-x)] [Medline: [35395724](https://pubmed.ncbi.nlm.nih.gov/35395724/)]
224. Palomino-Echeverria S, Huergo E, Ortega-Legarreta A, et al. A robust clustering strategy for stratification unveils unique patient subgroups in acutely decompensated cirrhosis. *J Transl Med*. Jun 27, 2024;22(1):599. [doi: [10.1186/s12967-024-05386-2](https://doi.org/10.1186/s12967-024-05386-2)] [Medline: [38937846](https://pubmed.ncbi.nlm.nih.gov/38937846/)]
225. Sinha A, Aljrees T, Pandey SK, et al. Semi-supervised clustering-based DANA algorithm for data gathering and disease detection in healthcare wireless sensor networks (WSN). *Sensors (Basel)*. Dec 19, 2023;24(1):18. [doi: [10.3390/s24010018](https://doi.org/10.3390/s24010018)] [Medline: [38202880](https://pubmed.ncbi.nlm.nih.gov/38202880/)]
226. Ren Z, Yeh RA, Schwing AG. Not all unlabeled data are equal: learning to weight data in semi-supervised learning. Presented at: 34th International Conference on Neural Information Processing System; Dec 6-12, 2020; Vancouver, BC, Canada. [doi: [10.5555/3495724.3497552](https://doi.org/10.5555/3495724.3497552)]
227. Huang L. Combination of information in labeled and unlabeled data via evidence theory. *IEEE Trans Artif Intell*. 2023;5(5):2179-2192. [doi: [10.1109/TAI.2023.3316194](https://doi.org/10.1109/TAI.2023.3316194)]
228. Qiu S, Chen Y, Yang Y, et al. A review on semi-supervised learning for EEG-based emotion recognition. *Information Fusion*. Apr 2024;104:102190. [doi: [10.1016/j.inffus.2023.102190](https://doi.org/10.1016/j.inffus.2023.102190)]
229. Christopoulou SC. Machine learning models and technologies for evidence-based telehealth and smart care: a review. *BioMedInformatics*. 2024;4(1):754-779. [doi: [10.3390/biomedinformatics4010042](https://doi.org/10.3390/biomedinformatics4010042)]
230. Naeem M, Rizvi STH, Coronato A. A gentle introduction to reinforcement learning and its application in different fields. *IEEE Access*. 2020;8:209320-209344. [doi: [10.1109/ACCESS.2020.3038605](https://doi.org/10.1109/ACCESS.2020.3038605)]
231. Sverdlov O, Ryznik Y, Wong WK. Opportunity for efficiency in clinical development: an overview of adaptive clinical trial designs and innovative machine learning tools, with examples from the cardiovascular field. *Contemp Clin Trials*. Jun 2021;105:106397. [doi: [10.1016/j.cct.2021.106397](https://doi.org/10.1016/j.cct.2021.106397)] [Medline: [33845209](https://pubmed.ncbi.nlm.nih.gov/33845209/)]
232. Kumar CUO, Singh I, Suguna M. Optimizing patient recruitment for clinical trials: a hybrid classification model and game-theoretic approach for strategic interaction. *IEEE Access*. 2024;12:10254-10280. [doi: [10.1109/ACCESS.2024.3351688](https://doi.org/10.1109/ACCESS.2024.3351688)]
233. Malheiro V, Santos B, Figueiras A, Mascarenhas-Melo F. The potential of artificial intelligence in pharmaceutical innovation: from drug discovery to clinical trials. *Pharmaceuticals (Basel)*. May 25, 2025;18(6):788. [doi: [10.3390/ph18060788](https://doi.org/10.3390/ph18060788)] [Medline: [40573185](https://pubmed.ncbi.nlm.nih.gov/40573185/)]
234. McKinney SM, Sieniek M, Godbole V, et al. International evaluation of an AI system for breast cancer screening. *Nature New Biol*. Jan 2, 2020;577(7788):89-94. [doi: [10.1038/s41586-019-1799-6](https://doi.org/10.1038/s41586-019-1799-6)]
235. Zhavoronkov A, Ivanenkov YA, Aliper A, et al. Deep learning enables rapid identification of potent DDR1 kinase inhibitors. *Nat Biotechnol*. Sep 2019;37(9):1038-1040. [doi: [10.1038/s41587-019-0224-x](https://doi.org/10.1038/s41587-019-0224-x)] [Medline: [31477924](https://pubmed.ncbi.nlm.nih.gov/31477924/)]
236. Adams R, Henry KE, Sridharan A, et al. Prospective, multi-site study of patient outcomes after implementation of the TREWS machine learning-based early warning system for sepsis. *Nat Med*. Jul 2022;28(7):1455-1460. [doi: [10.1038/s41591-022-01894-0](https://doi.org/10.1038/s41591-022-01894-0)] [Medline: [35864252](https://pubmed.ncbi.nlm.nih.gov/35864252/)]
237. Piening B, Bapat B, Weerasinghe RK, et al. Improved outcomes from reflex comprehensive genomic profiling-guided precision therapeutic selection across a major US healthcare system. *JCO*. Jun 1, 2023;41(16_suppl):6622-6622. [doi: [10.1200/JCO.2023.41.16_suppl.6622](https://doi.org/10.1200/JCO.2023.41.16_suppl.6622)]
238. Iyortsuun NK, Kim SH, Jhon M, Yang HJ, Pant S. A review of machine learning and deep learning approaches on mental health diagnosis. *Healthcare (Basel)*. Jan 17, 2023;11(3):285. [doi: [10.3390/healthcare11030285](https://doi.org/10.3390/healthcare11030285)] [Medline: [36766860](https://pubmed.ncbi.nlm.nih.gov/36766860/)]

239. Konečný J, McMahan HB, Ramage D, Richtárik P. Federated optimization: distributed machine learning for on-device intelligence. arXiv. Preprint posted online on Oct 8, 2016. URL: <https://arxiv.org/abs/1610.02527> [Accessed 2026-05-07]
240. Yang Q, Liu Y, Chen T, Tong Y. Federated machine learning: concept and applications. *ACM Transactions on Intelligent Systems and Technology*. 2019;10(2):1-19. [doi: [10.1145/3298981](https://doi.org/10.1145/3298981)]
241. Zhang X, Mavromatis A, Vafeas A, Nejabati R, Simeonidou D. Federated feature selection for horizontal federated learning in IoT networks. *IEEE Internet Things J*. 2023;10(11):10095-10112. [doi: [10.1109/JIOT.2023.3237032](https://doi.org/10.1109/JIOT.2023.3237032)]
242. Gao D, Ju C, Wei X, Liu Y, Chen T, Yang Q. HHHFL: hierarchical heterogeneous horizontal federated learning for electroencephalography. arXiv. Preprint posted online on Sep 11, 2019. URL: <https://arxiv.org/abs/1909.05784> [Accessed 2026-05-07]
243. Huang W, Li T, Wang D, Du S, Zhang J, Huang T. Fairness and accuracy in horizontal federated learning. *Inf Sci (Ny)*. Apr 2022;589:170-185. [doi: [10.1016/j.ins.2021.12.102](https://doi.org/10.1016/j.ins.2021.12.102)]
244. Liu Y, Kang Y, Zou T, et al. Vertical federated learning: concepts, advances, and challenges. *IEEE Trans Knowl Data Eng*. 2024;36(7):3615-3634. [doi: [10.1109/TKDE.2024.3352628](https://doi.org/10.1109/TKDE.2024.3352628)]
245. Feng S, Yu H, Zhu Y. MMVFL: a simple vertical federated learning framework for multi-class multi-participant scenarios. *Sensors (Basel)*. Jan 18, 2024;24(2):619. [doi: [10.3390/s24020619](https://doi.org/10.3390/s24020619)] [Medline: [38257712](https://pubmed.ncbi.nlm.nih.gov/38257712/)]
246. Gupta M, Sharma P, Kalra R. Federated learning and artificial intelligence in e-healthcare. In: Hassan A, Prasad VK, Bhattacharya P, Dutta P, Damaševičius R, editors. *Federated Learning and AI for Healthcare 5.0*. IGI Global; 2024:104-118. [doi: [10.4018/979-8-3693-1082-3.ch006](https://doi.org/10.4018/979-8-3693-1082-3.ch006)]
247. Liu Y, Kang Y, Xing C, Chen T, Yang Q. A secure federated transfer learning framework. *IEEE Intell Syst*. 2020;35(4):70-82. [doi: [10.1109/MIS.2020.2988525](https://doi.org/10.1109/MIS.2020.2988525)]
248. Chen Y, Qin X, Wang J, Yu C, Gao W. FedHealth: a federated transfer learning framework for wearable healthcare. *IEEE Intell Syst*. 2020;35(4):83-93. [doi: [10.1109/MIS.2020.2988604](https://doi.org/10.1109/MIS.2020.2988604)]
249. Chorney W, Wang H. Towards federated transfer learning in electrocardiogram signal analysis. *Comput Biol Med*. Mar 2024;170:107984. [doi: [10.1016/j.compbiomed.2024.107984](https://doi.org/10.1016/j.compbiomed.2024.107984)] [Medline: [38244469](https://pubmed.ncbi.nlm.nih.gov/38244469/)]
250. Rieke N, Hancox J, Li W, et al. The future of digital health with federated learning. *NPJ Digit Med*. 2020;3(1):119. [doi: [10.1038/s41746-020-00323-1](https://doi.org/10.1038/s41746-020-00323-1)] [Medline: [33015372](https://pubmed.ncbi.nlm.nih.gov/33015372/)]
251. Nguyen DC, Pham QV, Pathirana PN, et al. Federated learning for smart healthcare: a survey. *ACM Comput Surv*. Mar 31, 2023;55(3):1-37. [doi: [10.1145/3501296](https://doi.org/10.1145/3501296)]
252. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. *IEEE Signal Process Mag*. 2020;37(3):50-60. [doi: [10.1109/MSP.2020.2975749](https://doi.org/10.1109/MSP.2020.2975749)]
253. Heyndrickx W, Mervin L, Morawietz T, et al. MELLODDY: cross-pharma federated learning at unprecedented scale unlocks benefits in QSAR without compromising proprietary information. *J Chem Inf Model*. Apr 8, 2024;64(7):2331-2344. [doi: [10.1021/acs.jcim.3c00799](https://doi.org/10.1021/acs.jcim.3c00799)] [Medline: [37642660](https://pubmed.ncbi.nlm.nih.gov/37642660/)]
254. Foley P, Sheller MJ, Edwards B, et al. OpenFL: the open federated learning library. *Phys Med Biol*. Oct 19, 2022;67(21):214001. [doi: [10.1088/1361-6560/ac97d9](https://doi.org/10.1088/1361-6560/ac97d9)] [Medline: [36198326](https://pubmed.ncbi.nlm.nih.gov/36198326/)]
255. Mora A, Bujari A, Bellavista P. Enhancing generalization in federated learning with heterogeneous data: a comparative literature review. *Future Generation Computer Systems*. Aug 2024;157:1-15. [doi: [10.1016/j.future.2024.03.027](https://doi.org/10.1016/j.future.2024.03.027)]
256. Almanifi ORA, Chow CO, Tham ML, Chuah JH, Kanesan J. Communication and computation efficiency in federated learning: a survey. *Internet of Things*. Jul 2023;22:100742. [doi: [10.1016/j.iot.2023.100742](https://doi.org/10.1016/j.iot.2023.100742)]
257. Dhatteval JS, Malik K, Kaswan KS, Elngar AA. Federated learning: overview, challenges, and ethical considerations. In: Elngar AA, Oliva D, Balas VE, editors. *Artificial Intelligence Using Federated Learning*. CRC Press; 2024:1-15. [doi: [10.1201/9781003482000-1](https://doi.org/10.1201/9781003482000-1)]
258. Mohammadi S, Balador A, Sinaei S, Flammini F. Balancing privacy and performance in federated learning: a systematic literature review on methods and metrics. *J Parallel Distrib Comput*. Oct 2024;192:104918. [doi: [10.1016/j.jpdc.2024.104918](https://doi.org/10.1016/j.jpdc.2024.104918)]
259. Saha S, Hota A, Chattopadhyay AK, Nag A, Nandi S. A multifaceted survey on privacy preservation of federated learning: progress, challenges, and opportunities. *Artif Intell Rev*. 2024;57(7):184. [doi: [10.1007/s10462-024-10766-7](https://doi.org/10.1007/s10462-024-10766-7)]
260. Narula M, Meena J, Vishwakarma DK. A comprehensive review on federated learning for data-sensitive application: open issues & challenges. *Eng Appl Artif Intell*. Jul 2024;133:108128. [doi: [10.1016/j.engappai.2024.108128](https://doi.org/10.1016/j.engappai.2024.108128)]
261. Malik H, Anees T. Federated learning with deep convolutional neural networks for the detection of multiple chest diseases using chest x-rays. *Multimed Tools Appl*. 2024;83(23):63017-63045. [doi: [10.1007/s11042-023-18065-z](https://doi.org/10.1007/s11042-023-18065-z)]
262. Dasaradharami Reddy K, Gadekallu TR. A comprehensive survey on federated learning techniques for healthcare informatics. *Comput Intell Neurosci*. 2023;2023(1):8393990. [doi: [10.1155/2023/8393990](https://doi.org/10.1155/2023/8393990)] [Medline: [36909974](https://pubmed.ncbi.nlm.nih.gov/36909974/)]
263. Kaissis GA, Makowski MR, Rückert D, Braren RF. Secure, privacy-preserving and federated machine learning in medical imaging. *Nat Mach Intell*. 2020;2(6):305-311. [doi: [10.1038/s42256-020-0186-1](https://doi.org/10.1038/s42256-020-0186-1)]
264. Rafi TH, Noor FA, Hussain T, Chae DK. Fairness and privacy preserving in federated learning: a survey. *Information Fusion*. May 2024;105:102198. [doi: [10.1016/j.inffus.2023.102198](https://doi.org/10.1016/j.inffus.2023.102198)]

265. Djebrouni Y, Benarba N, Touat O, et al. Bias mitigation in federated learning for edge computing. *Proc ACM Interact Mob Wearable Ubiquitous Technol.* Dec 19, 2023;7(4):1-35. [doi: [10.1145/3631455](https://doi.org/10.1145/3631455)]
266. You L, Guo Z, Zuo B, Chang Y, Yuen C. SLMFed: a stage-based and layerwise mechanism for incremental federated learning to assist dynamic and ubiquitous IoT. *IEEE Internet Things J.* 2024;11(9):16364-16381. [doi: [10.1109/JIOT.2024.3353793](https://doi.org/10.1109/JIOT.2024.3353793)]
267. Mazzocca C, Romandini N, Montanari R, Bellavista P. Enabling federated learning at the edge through the IOTA tangle. *Future Generation Computer Systems.* Mar 2024;152:17-29. [doi: [10.1016/j.future.2023.10.014](https://doi.org/10.1016/j.future.2023.10.014)]
268. Ji J, Shu Z, Li H, et al. Edge-computing-based knowledge distillation and multitask learning for partial discharge recognition. *IEEE Trans Instrum Meas.* 2024;73:1-11. [doi: [10.1109/TIM.2024.3351239](https://doi.org/10.1109/TIM.2024.3351239)]
269. Elhattab F, Bouchenak S, Boscher C. PASTEL: privacy-preserving federated learning in edge computing. *Proc ACM Interact Mob Wearable Ubiquitous Technol.* 2024;7(4):1-29. [doi: [10.1145/3633808](https://doi.org/10.1145/3633808)]
270. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Bitcoin.org*; 2008. URL: <https://bitcoin.org/bitcoin.pdf> [Accessed 2026-05-07]
271. Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum*; 2025. URL: <https://ethereum.github.io/yellowpaper/paper.pdf> [Accessed 2026-06-01]
272. Dutta P, Choi TM, Somani S, Butala R. Blockchain technology in supply chain operations: applications, challenges and research opportunities. *Transp Res E Logist Transp Rev.* Oct 2020;142:102067. [doi: [10.1016/j.tre.2020.102067](https://doi.org/10.1016/j.tre.2020.102067)] [Medline: [33013183](https://pubmed.ncbi.nlm.nih.gov/33013183/)]
273. Casado-Vara R, Prieto J, la Prieta FD, Corchado JM. How blockchain improves the supply chain: case study alimentary supply chain. *Procedia Comput Sci.* 2018;134:393-398. [doi: [10.1016/j.procs.2018.07.193](https://doi.org/10.1016/j.procs.2018.07.193)]
274. Korpela K, Hallikas J, Dahlberg T. Digital supply chain transformation toward blockchain integration. Presented at: 50th Hawaii International Conference on System Sciences; Jan 4-7, 2017; Big Island, HI, USA. [doi: [10.24251/HICSS.2017.506](https://doi.org/10.24251/HICSS.2017.506)]
275. Queiroz MM, Telles R, Bonilla SH. Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management.* Aug 22, 2019;25(2):241-254. [doi: [10.1108/SCM-03-2018-0143](https://doi.org/10.1108/SCM-03-2018-0143)]
276. Raval S. *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology.* O'Reilly Media, Inc; 2016. [doi: [10.5555/3074145](https://doi.org/10.5555/3074145)]
277. Joshi AP, Han M, Wang Y. A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing.* 2018;1(2):121-147. [doi: [10.3934/mfc.2018007](https://doi.org/10.3934/mfc.2018007)]
278. Mohanta BK, Jena D, Panda SS, Sobhanayak S. Blockchain technology: a survey on applications and security privacy challenges. *Internet of Things.* Dec 2019;8:100107. [doi: [10.1016/j.iot.2019.100107](https://doi.org/10.1016/j.iot.2019.100107)]
279. Ul Hassan M, Rehmani MH, Chen J. Anomaly detection in blockchain networks: a comprehensive survey. *IEEE Commun Surv Tutor.* 2022;25(1):289-318. [doi: [10.1109/COMST.2022.3205643](https://doi.org/10.1109/COMST.2022.3205643)]
280. Shahsavari Y, Zhang K, Talhi C. A theoretical model for block propagation analysis in bitcoin network. *IEEE Trans Eng Manage.* 2020;69(4):1459-1476. [doi: [10.1109/TEM.2020.2989170](https://doi.org/10.1109/TEM.2020.2989170)]
281. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: past, present, and future trends. *ACM Comput Surv.* Nov 30, 2022;54(8):1-41. [doi: [10.1145/3471140](https://doi.org/10.1145/3471140)]
282. Lafourcade P, Lombard-Platet M. About blockchain interoperability. *Inf Process Lett.* Sep 2020;161:105976. [doi: [10.1016/j.ipl.2020.105976](https://doi.org/10.1016/j.ipl.2020.105976)]
283. Schulte S, Sigwart M, Frauenthaler P, Borkowski M. Towards blockchain interoperability. In: Di Ciccio C, editor. *Business Process Management: Blockchain and Central and Eastern Europe Forum BPM 2019 Lecture Notes in Business Information Processing.* Springer; 2019:3-10. [doi: [10.1007/978-3-030-30429-4_1](https://doi.org/10.1007/978-3-030-30429-4_1)]
284. Hardjono T, Lipton A, Pentland A. Toward an interoperability architecture for blockchain autonomous systems. *IEEE Trans Eng Manage.* 2019;67(4):1298-1309. [doi: [10.1109/TEM.2019.2920154](https://doi.org/10.1109/TEM.2019.2920154)]
285. Zhang P, White J, Schmidt DC, Lenz G. Applying software patterns to address interoperability in blockchainbased healthcare apps. *arXiv.* Preprint posted online on Jun 5, 2017. URL: <https://arxiv.org/abs/1706.03700> [Accessed 2026-05-07]
286. Qasse IA, Abu Talib M, Nasir Q. Inter blockchain communication. Presented at: 6th Annual International Conference Research Track; Mar 7-9, 2019; Rabat, Morocco. [doi: [10.1145/3333165.3333167](https://doi.org/10.1145/3333165.3333167)]
287. Zou W, Lo D, Kochhar PS, et al. Smart contract development: challenges and opportunities. *IEEE Trans Software Eng.* 2019;47(10):2084-2106. [doi: [10.1109/TSE.2019.2942301](https://doi.org/10.1109/TSE.2019.2942301)]
288. Delmolino K, Arnett M, Kosba A, Miller A, Shi E. Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In: Clark J, Meiklejohn S, Ryan P, Wallach D, Brenner M, Rohloff K, editors. *Financial Cryptography and Data Security FC 2016 Lecture Notes in Computer Science.* Springer; 2016:79-94. [doi: [10.1007/978-3-662-53357-4_6](https://doi.org/10.1007/978-3-662-53357-4_6)]
289. Xu J, Wang C, Jia X. A survey of blockchain consensus protocols. *ACM Comput Surv.* Dec 31, 2023;55(13s):1-35. [doi: [10.1145/3579845](https://doi.org/10.1145/3579845)]
290. Nguyen GT, Kim K. A survey about consensus algorithms used in blockchain. *J Inf Process Syst.* 2018;14(1):101-128. [doi: [10.3745/JIPS.01.0024](https://doi.org/10.3745/JIPS.01.0024)]

291. Monrat AA, Schelen O, Andersson K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*. 2019;7:117134-117151. [doi: [10.1109/ACCESS.2019.2936094](https://doi.org/10.1109/ACCESS.2019.2936094)]
292. Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. Presented at: 2016 ACM SIGSAC Conference on Computer and Communications Security; Oct 24-28, 2016; Vienna, Austria. [doi: [10.1145/2976749.2978341](https://doi.org/10.1145/2976749.2978341)]
293. Shahsavari Y, Zhang K, Talhi C. A theoretical model for fork analysis in the bitcoin network. Presented at: 2019 IEEE International Conference on Blockchain (Blockchain); Jul 14-17, 2019; Atlanta, GA, USA. [doi: [10.1109/Blockchain.2019.00038](https://doi.org/10.1109/Blockchain.2019.00038)]
294. Nguyen CT, Hoang DT, Nguyen DN, Niyato D, Nguyen HT, Dutkiewicz E. Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*. 2019;7:85727-85745. [doi: [10.1109/ACCESS.2019.2925010](https://doi.org/10.1109/ACCESS.2019.2925010)] [Medline: [33777591](https://pubmed.ncbi.nlm.nih.gov/33777591/)]
295. Buterin V. A next-generation smart contract and decentralized application platform. Ethereum; 2014. URL: https://cryptorating.eu/whitepapers/Ethereum/Ethereum_white_paper.pdf [Accessed 2026-06-01]
296. Introduction. Cardano Documentation. URL: <https://docs.cardano.org/introduction> [Accessed 2024-02-22]
297. Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling byzantine agreements for cryptocurrencies. Presented at: 26th Symposium on Operating Systems Principles; Oct 28, 2017; Shanghai, China. [doi: [10.1145/3132747.3132757](https://doi.org/10.1145/3132747.3132757)]
298. Wang Q, Xu M, Li X, Qian H. Revisiting the fairness and randomness of delegated proof of stake consensus algorithm. Presented at: 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom); Dec 17-19, 2020; Exeter, United Kingdom. [doi: [10.1109/ISPA-BDCLOUD-SocialCom-SustainCom51426.2020.00064](https://doi.org/10.1109/ISPA-BDCLOUD-SocialCom-SustainCom51426.2020.00064)]
299. Lamport L, Shostak R, Pease M. The Byzantine generals problem. In: Malkhi D, editor. *Concurrency: The Works of Leslie Lamport*. 2019:203-226. [doi: [10.1145/3335772.3335936](https://doi.org/10.1145/3335772.3335936)]
300. Zhong W, Yang C, Liang W, et al. Byzantine fault-tolerant consensus algorithms: a survey. *Electronics (Basel)*. 2023;12(18):3801. [doi: [10.3390/electronics12183801](https://doi.org/10.3390/electronics12183801)]
301. Shahsavari Y, Zhang K, Talhi C. Performance modeling and analysis of hotstuff for blockchain consensus. Presented at: Fourth International Conference on Blockchain Computing and Applications (BCCA); Sep 5-7, 2022; San Antonio, TX, USA. [doi: [10.1109/BCCA55292.2022.9922238](https://doi.org/10.1109/BCCA55292.2022.9922238)]
302. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. Presented at: Thirteenth EuroSys Conference; Apr 23-26, 2018; Porto, Portugal. [doi: [10.1145/3190508.3190538](https://doi.org/10.1145/3190508.3190538)]
303. Li Y, Cao B, Peng M, et al. Direct acyclic graph-based ledger for Internet of Things: performance and security analysis. *IEEE/ACM Trans Networking*. 2020;28(4):1643-1656. [doi: [10.1109/TNET.2020.2991994](https://doi.org/10.1109/TNET.2020.2991994)]
304. Popov S. The tangle. *Semantic Scholar*. 2018. URL: <https://www.semanticscholar.org/paper/The-Tangle-Popov/43586b34b054b48891d478407d4e7435702653e0> [Accessed 2026-05-07]
305. Saa O, Cullen A, Vigneri L. IOTA 2.0 incentives and tokenomics whitepaper. IOTA; 2023. URL: https://files.iota.org/papers/IOTA_2.0_Incentives_And-Tokenomics_Whitepaper.pdf [Accessed 2026-05-07]
306. Pass R, Shi E. Hybrid consensus: efficient consensus in the permissionless model. *Cryptology ePrint Archive*. 2016. URL: <https://eprint.iacr.org/2016/917> [Accessed 2026-05-07]
307. Chepurnoy A, Duong T, Fan L, Zhou HS. Twinscoin: a cryptocurrency via proof-of-work and proof-of-stake. *Cryptology ePrint Archive*. 2017. URL: <https://eprint.iacr.org/2017/232> [Accessed 2026-05-07]
308. Kwon J. Tendermint: consensus without mining. *Tendermint*; 2014. URL: <https://tendermint.com/static/docs/tendermint.pdf> [Accessed 2026-05-07]
309. Cheng Z, Wu G, Wu H, Zhao M, Zhao L, Cai Q. A new hybrid consensus protocol: deterministic proof of work. *arXiv Preprint* posted online on Aug 13, 2018. URL: <https://arxiv.org/abs/1808.04142> [Accessed 2026-05-07]
310. Jayakumari B, Sheeba SL, Eapen M, et al. E-voting system using cloud-based hybrid blockchain technology. *J Saf Sci Resil*. Mar 2024;5(1):102-109. [doi: [10.1016/j.jnlssr.2024.01.002](https://doi.org/10.1016/j.jnlssr.2024.01.002)]
311. Zarrin J, Wen Phang H, Babu Saheer L, Zarrin B. Blockchain for decentralization of internet: prospects, trends, and challenges. *Cluster Comput*. 2021;24(4):2841-2866. [doi: [10.1007/s10586-021-03301-8](https://doi.org/10.1007/s10586-021-03301-8)] [Medline: [34025209](https://pubmed.ncbi.nlm.nih.gov/34025209/)]
312. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, Wang J. Untangling blockchain: a data processing view of blockchain systems. *IEEE Trans Knowl Data Eng*. 2018;30(7):1366-1385. [doi: [10.1109/TKDE.2017.2781227](https://doi.org/10.1109/TKDE.2017.2781227)]
313. Decker C, Wattenhofer R. Information propagation in the bitcoin network. Presented at: International Conference on Peer-to-Peer Computing; Sep 9-11, 2013; Trento, Italy. [doi: [10.1109/P2P.2013.6688704](https://doi.org/10.1109/P2P.2013.6688704)]
314. Kan L, Wei Y, Hafiz Muhammad A, Siyuan W, Gao LC, Kai H. A multiple blockchains architecture on inter-blockchain communication. Presented at: 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C); Jul 16-20, 2018; Lisbon, Portugal. [doi: [10.1109/QRS-C.2018.00037](https://doi.org/10.1109/QRS-C.2018.00037)]
315. Chen Z dong, Yu Z, Duan Z bo, Hu K. Inter-blockchain communication. *DEStech Transactions on Computer Science and Engineering*. 2017:12539. [doi: [10.12783/dtcese/cst2017/12539](https://doi.org/10.12783/dtcese/cst2017/12539)]

316. Tam Vo H, Wang Z, Karunamoorthy D, Wagner J, Abebe E, Mohania M. Internet of blockchains: techniques and challenges ahead. Presented at: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); Jul 30 to Aug 3, 2018; Halifax, NS, Canada. [doi: [10.1109/Cybermatics.2018.2018.00264](https://doi.org/10.1109/Cybermatics.2018.2018.00264)]
317. Kwon J, Buchman E. Cosmos: a network of distributed ledgers. GitHub. URL: <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md> [Accessed 2026-05-07]
318. Wood G. Polkadot: vision for a heterogeneous multi-chain framework. Polkadot; 2016. URL: <https://assets.polkadot.network/Polkadot-whitepaper.pdf> [Accessed 2026-05-07]
319. Wanchain. URL: <https://www.wanchain.org/> [Accessed 2024-03-11]
320. Mahajan HB, Junnarkar AA. Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimed Tools Appl*. Apr 15, 2023;82(28):1-24. [doi: [10.1007/s11042-023-15204-4](https://doi.org/10.1007/s11042-023-15204-4)] [Medline: [37362704](https://pubmed.ncbi.nlm.nih.gov/37362704/)]
321. Pahlajani S, Kshirsagar A, Pachghare V. Survey on private blockchain consensus algorithms. Presented at: 1st International Conference on Innovations in Information and Communication Technology (ICIICT); Apr 25-26, 2019; Chennai, India. [doi: [10.1109/ICIICT1.2019.8741353](https://doi.org/10.1109/ICIICT1.2019.8741353)]
322. Antwi M, Adnane A, Ahmad F, Hussain R, Habib ur Rehman M, Kerrache CA. The case of HyperLedger fabric as a blockchain solution for healthcare applications. *Blockchain: Research and Applications*. Mar 2021;2(1):100012. [doi: [10.1016/j.bcra.2021.100012](https://doi.org/10.1016/j.bcra.2021.100012)]
323. Al-Sumaidae G, Alkhudary R, Zilic Z, Swidan A. Performance analysis of a private blockchain network built on hyperledger fabric for healthcare. *Inf Process Manag*. Mar 2023;60(2):103160. [doi: [10.1016/j.ipm.2022.103160](https://doi.org/10.1016/j.ipm.2022.103160)]
324. Irresberger F, John K, Mueller P, Saleh F. The public blockchain ecosystem: an empirical analysis. NYU Stern School of Business; 2020. [doi: [10.2139/ssrn.3592849](https://doi.org/10.2139/ssrn.3592849)]
325. Ferdous MS, Chowdhury MJM, Hoque MA. A survey of consensus algorithms in public blockchain systems for cryptocurrencies. *J Netw Comput Appl*. May 2021;182:103035. [doi: [10.1016/j.jnca.2021.103035](https://doi.org/10.1016/j.jnca.2021.103035)]
326. Benhamouda F, Gentry C, Gorbunov S, et al. Can a public blockchain keep a secret? In: Pass R, Pietrzak K, editors. *Theory of Cryptography TCC 2020 Lecture Notes in Computer Science*. Springer; 2020:260-290. [doi: [10.1007/978-3-030-64375-1_10](https://doi.org/10.1007/978-3-030-64375-1_10)]
327. Rebello GAF, Camilo GF, de Souza LAC, et al. A survey on blockchain scalability: from hardware to layer-two protocols. *IEEE Commun Surv Tutor*. 2024;26(4):2411-2458. [doi: [10.1109/COMST.2024.3376252](https://doi.org/10.1109/COMST.2024.3376252)]
328. Dib O, Brousmiche KL, Durand A, Thea E, Hamida EB. Consortium blockchains: overview, applications and challenges. *Int J Adv Telecommun*. 2018;11(1):51-64. URL: https://personales.upv.es/thinkmind/Tele/Tele_v11_n12_2018/tele_v11_n12_2018_5.html [Accessed 2026-05-07]
329. Li Z, Kang J, Yu R, Ye D, Deng Q, Zhang Y. Consortium blockchain for secure energy trading in industrial Internet of Things. *IEEE Trans Ind Inf*. 2017;14(8):1-1. [doi: [10.1109/TII.2017.2786307](https://doi.org/10.1109/TII.2017.2786307)]
330. Yao W, Ye J, Murimi R, Wang G. A survey on consortium blockchain consensus mechanisms. arXiv. Preprint posted online on Feb 24, 2021. URL: <https://arxiv.org/abs/2102.12058v2> [Accessed 2026-05-07]
331. Zhang A, Lin X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J Med Syst*. Jun 28, 2018;42(8):140. [doi: [10.1007/s10916-018-0995-5](https://doi.org/10.1007/s10916-018-0995-5)] [Medline: [29956061](https://pubmed.ncbi.nlm.nih.gov/29956061/)]
332. Li D, Han D, Weng TH, et al. Blockchain for federated learning toward secure distributed machine learning systems: a systemic survey. *Soft Comput*. 2022;26(9):4423-4440. [doi: [10.1007/s00500-021-06496-5](https://doi.org/10.1007/s00500-021-06496-5)] [Medline: [34840525](https://pubmed.ncbi.nlm.nih.gov/34840525/)]
333. Houda ZAE, Hafid AS, Khoukhi L, Brik B. When collaborative federated learning meets blockchain to preserve privacy in healthcare. *IEEE Trans Netw Sci Eng*. 2022;10(5):2455-2465. [doi: [10.1109/TNSE.2022.3211192](https://doi.org/10.1109/TNSE.2022.3211192)]
334. Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z. Blockchain-based federated learning for securing Internet of Things: a comprehensive survey. *ACM Comput Surv*. Sep 30, 2023;55(9):1-43. [doi: [10.1145/3560816](https://doi.org/10.1145/3560816)]
335. Passerat-Palmbach J, Farnan T, McCoy M, et al. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. Presented at: 2020 IEEE International Conference on Blockchain (Blockchain); Nov 2-6, 2020; Rhodes, Greece. [doi: [10.1109/Blockchain50366.2020.00080](https://doi.org/10.1109/Blockchain50366.2020.00080)]
336. Aich S, Sinai NK, Kumar S, et al. Protecting personal healthcare record using blockchain & federated learning technologies. Presented at: 24th International Conference on Advanced Communication Technology (ICACT); Feb 13-16, 2022; PyeongChang Kwangwoon_Do, Korea, Republic of. [doi: [10.23919/ICACT53585.2022.9728772](https://doi.org/10.23919/ICACT53585.2022.9728772)]
337. El Rifai O, Biotteau M, de Boissezon X, Megdiche I, Ravat F, Teste O. Blockchain-based federated learning in medicine. In: Michalowski M, Moskovitch R, editors. *Artificial Intelligence in Medicine AIME 2020 Lecture Notes in Computer Science*. Springer; 2020:214-224. [doi: [10.1007/978-3-030-59137-3_20](https://doi.org/10.1007/978-3-030-59137-3_20)]
338. Kim YJ, Hong CS. Blockchain-based node-aware dynamic weighting methods for improving federated learning performance. Presented at: 20th Asia-Pacific Network Operations and Management Symposium (APNOMS); Sep 18-20, 2019; Matsue, Japan. [doi: [10.23919/APNOMS.2019.8893114](https://doi.org/10.23919/APNOMS.2019.8893114)]
339. Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet Things J*. 2020;8(4):2276-2288. [doi: [10.1109/JIOT.2020.3015772](https://doi.org/10.1109/JIOT.2020.3015772)]

340. Pandey SR, Nguyen LD, Popovski P. FedToken: tokenized incentives for data contribution in federated learning. arXiv. Preprint posted online on Sep 20, 2022. URL: <https://arxiv.org/abs/2209.09775> [Accessed 2026-05-07]
341. Behera MR, Upadhyay S, Shetty S. Federated learning using smart contracts on blockchains, based on reward driven approach. arXiv. Preprint posted online on Jul 19, 2021. URL: <https://arxiv.org/abs/2107.10243> [Accessed 2026-05-07]
342. Ma S, Cao Y, Xiong L. Transparent contribution evaluation for secure federated learning on blockchain. Presented at: 37th International Conference on Data Engineering Workshops (ICDEW); Apr 19-22, 2021; Chania, Greece. [doi: [10.1109/ICDEW53142.2021.00023](https://doi.org/10.1109/ICDEW53142.2021.00023)]
343. Wang Z, Hu Q. Blockchain-based federated learning: a comprehensive survey. arXiv. Preprint posted online on Oct 5, 2021. URL: <https://arxiv.org/abs/2110.02182v1> [Accessed 2026-05-07]
344. Munusamy S, Jothi KR. Blockchain-enabled federated learning with edge analytics for secure and efficient electronic health records management. *Sci Rep.* Jul 28, 2025;15(1):27524. [doi: [10.1038/s41598-025-12225-x](https://doi.org/10.1038/s41598-025-12225-x)] [Medline: [40721766](https://pubmed.ncbi.nlm.nih.gov/40721766/)]
345. Castro M, Liskov B. Practical Byzantine fault tolerance. Presented at: Third Symposium on Operating Systems Design and Implementation; Feb 22-25, 1999; New Orleans, LA, USA. [doi: [10.5555/296806.296824](https://doi.org/10.5555/296806.296824)]
346. Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. *ACM Trans Comput Syst.* Nov 2002;20(4):398-461. [doi: [10.1145/571637.571640](https://doi.org/10.1145/571637.571640)]
347. McMahan B, McMahan E, Ramage D, Hampson S, Aguera y Arcas B. Communication-efficient learning of deep networks from decentralized data. In: *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*. PMLR; 2017:1273-1282. URL: <https://proceedings.mlr.press/v54/mcmahan17a> [Accessed 2026-05-07]
348. Buchman E. Tendermint: Byzantine fault tolerance in the age of blockchains [Dissertation]. University of Guelph; 2016. URL: <https://atrium.lib.uoguelph.ca/items/5459099e-67aa-4a23-83ae-d3471d8d8336> [Accessed 2026-05-07]
349. Hu K, Gong S, Zhang Q, Seng C, Xia M, Jiang S. An overview of implementing security and privacy in federated learning. *Artif Intell Rev.* 2024;57(8):204. [doi: [10.1007/s10462-024-10846-8](https://doi.org/10.1007/s10462-024-10846-8)]
350. Xie M, Zhang Z, Hong H, Zhang G, Qin Y. Secure medical data sharing featuring traceable data usage and automatic audit mechanism. *IEEE Internet Things J.* 2025;12(13):25587-25600. [doi: [10.1109/JIOT.2025.3559926](https://doi.org/10.1109/JIOT.2025.3559926)]
351. Li C, Xing Z, Liu J, et al. Integrating zero-knowledge proofs into federated learning: a path to on-chain verifiable and privacy-preserving federated learning frameworks. *Int J Web Inf Syst.* May 15, 2025;21(3):275-297. [doi: [10.1108/IJWIS-01-2025-0024](https://doi.org/10.1108/IJWIS-01-2025-0024)]
352. Han B, Li B, Jurdak R, et al. PBFL: a privacy-preserving blockchain-based federated learning framework with homomorphic encryption and single masking. *IEEE Internet Things J.* 2025;12(10):14229-14243. [doi: [10.1109/JIOT.2024.3524632](https://doi.org/10.1109/JIOT.2024.3524632)]
353. Lavin R, Liu X, Mohanty H, Norman L, Zaarour G, Krishnamachari B. A survey on the applications of zero-knowledge proofs. arXiv. Preprint posted online on Aug 1, 2024. URL: <https://arxiv.org/abs/2408.00243> [Accessed 2026-05-07]
354. Zhou Z, Li Y, Wang Y, et al. ZHE: efficient zero-knowledge proofs for HE evaluations. Presented at: 2025 IEEE Symposium on Security and Privacy (SP); May 12-15, 2025; San Francisco, CA, USA. [doi: [10.1109/SP61157.2025.00199](https://doi.org/10.1109/SP61157.2025.00199)]
355. Wang X, Chen T, Dai HN, et al. A privacy-enhanced method for privacy-preserving and verifiable federated learning. *IEEE Internet Things J.* 2025;12(14):26768-26781. [doi: [10.1109/JIOT.2025.3561262](https://doi.org/10.1109/JIOT.2025.3561262)]
356. Munjal K, Bhatia R. A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex Intell Syst.* Aug 2023;9(4):3759-3786. [doi: [10.1007/s40747-022-00756-z](https://doi.org/10.1007/s40747-022-00756-z)]
357. Kalapaaking AP, Stephanie V, Khalil I, Atiquzzaman M, Yi X, Almashor M. SMPC-based federated learning for 6G-enabled Internet of Medical Things. *IEEE Netw.* 2022;36(4):182-189. [doi: [10.1109/MNET.007.2100717](https://doi.org/10.1109/MNET.007.2100717)]
358. Liu F, Zheng Z, Shi Y, Tong Y, Zhang Y. A survey on federated learning: a perspective from multi-party computation. *Front Comput Sci.* Feb 2024;18(1):181336. [doi: [10.1007/s11704-023-3282-7](https://doi.org/10.1007/s11704-023-3282-7)]
359. Naresh VS, Venkata Raju A, Srinivasa Rao O. Secure multiparty computation for privacy-preserving machine learning in healthcare: a comprehensive survey. *WIREs Computational Stats.* Sep 2025;17(3):e70046. URL: <https://wires.onlinelibrary.wiley.com/toc/19390068/17/3> [doi: [10.1002/wics.70046](https://doi.org/10.1002/wics.70046)]
360. Hosseini SM, Sikaroudi M, Babaei M, Tizhoosh HR. Cluster based secure multi-party computation in federated learning for histopathology images. In: Albarqouni S, editor. *Distributed, Collaborative, and Federated Learning, and Affordable AI and Healthcare for Resource Diverse Global Health DeCaF FAIR 2022 2022 Lecture Notes in Computer Science*. Springer; 2022:110-118. [doi: [10.1007/978-3-031-18523-6_11](https://doi.org/10.1007/978-3-031-18523-6_11)]
361. Kalapaaking AP, Khalil I, Rahman MS, Atiquzzaman M, Yi X, Almashor M. Blockchain-based federated learning with secure aggregation in trusted execution environment for Internet-of-Things. *IEEE Trans Ind Inf.* 2023;19(2):1703-1714. [doi: [10.1109/TII.2022.3170348](https://doi.org/10.1109/TII.2022.3170348)]
362. Zhu L, Hu S, Zhu X, Meng C, Huang M. Enhancing the security and privacy in the IoT supply chain using blockchain and federated learning with trusted execution environment. *Mathematics.* 2023;11(17):3759. [doi: [10.3390/math11173759](https://doi.org/10.3390/math11173759)]

363. Jiang J, Soriente C, Karame G. On the challenges of detecting side-channel attacks in SGX. Presented at: 25th International Symposium on Research in Attacks, Intrusions and Defenses; Oct 26-28, 2022; Limassol, Cyprus. [doi: [10.1145/3545948.3545972](https://doi.org/10.1145/3545948.3545972)]
364. Guo J, Vaswani K, Paverd A, Pietzuch P. VerifiableFL: verifiable claims for federated learning using exclaves. arXiv. Preprint posted online on Dec 13, 2025. URL: <https://arxiv.org/abs/2412.10537> [Accessed 2026-05-07]
365. Zhang L, Fang G, Tan Z. FedCCW: a privacy-preserving Byzantine-robust federated learning with local differential privacy for healthcare. *Cluster Comput*. Jun 2025;28(3):182. [doi: [10.1007/s10586-024-04894-6](https://doi.org/10.1007/s10586-024-04894-6)]
366. Tayyeh HK, AL-Jumaili ASA. Balancing privacy and performance: a differential privacy approach in federated learning. *Computers*. 2024;13(11):277. [doi: [10.3390/computers13110277](https://doi.org/10.3390/computers13110277)]
367. Shukla S, Rajkumar S, Sinha A, Esha M, Elango K, Sampath V. Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity. *Sci Rep*. Apr 16, 2025;15(1):13061. [doi: [10.1038/s41598-025-95858-2](https://doi.org/10.1038/s41598-025-95858-2)] [Medline: [40240790](https://pubmed.ncbi.nlm.nih.gov/40240790/)]
368. Cao X, Fang M, Liu J, Gong NZ. FLTrust: Byzantine-robust federated learning via trust bootstrapping. Presented at: NDSS Symposium 2021 Program; Feb 21-25, 2021; Virtual. [doi: [10.14722/ndss.2021.24434](https://doi.org/10.14722/ndss.2021.24434)]
369. Yan G, Wang H, Yuan X, Li J. DeFL: defending against model poisoning attacks in federated learning via critical learning periods awareness. *AAAI*. 2023;37(9):10711-10719. [doi: [10.1609/aaai.v37i9.26271](https://doi.org/10.1609/aaai.v37i9.26271)]
370. Bagdasaryan E, Veit A, Hua Y, Estrin D, Shmatikov V. How to backdoor federated learning. In: *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*. PMLR; 2020:2938-2948. URL: <https://proceedings.mlr.press/v108/bagdasaryan20a.html> [Accessed 2026-05-07]
371. Xie C, Chen M, Chen PY, Li B. CRFL: certifiably robust federated learning against backdoor attacks. In: *Proceedings of the 38th International Conference on Machine Learning*. PMLR; 2021:11372-11382. URL: <https://proceedings.mlr.press/v139/xie21a.html> [Accessed 2026-05-07]
372. Geiping J, Bauermeister H, Droge H, Moeller M. Inverting gradients—how easy is it to break privacy in federated learning? In: *Advances in Neural Information Processing Systems 33 (NeurIPS 2020)*. NeurIPS; 2020:16937-16947. URL: <https://proceedings.neurips.cc/paper/2020/hash/c4ede56bbd98819ae6112b20ac6bf145-Abstract.html> [Accessed 2026-05-07]
373. Hatamizadeh A, Yin H, Roth H, et al. GradViT: gradient inversion of vision transformers. Presented at: 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR); Jun 18-24, 2022; New Orleans, LA, USA. [doi: [10.1109/CVPR52688.2022.00978](https://doi.org/10.1109/CVPR52688.2022.00978)]
374. Geng J, Mou Y, Li Q, et al. Improved gradient inversion attacks and defenses in federated learning. *IEEE Trans Big Data*. 2024;10(6):839-850. [doi: [10.1109/TBDDATA.2023.3239116](https://doi.org/10.1109/TBDDATA.2023.3239116)]
375. Nguyen T, Lai P, Tran K, Phan N, Thai MT. Active membership inference attack under local differential privacy in federated learning. In: *Proceedings of The 26th International Conference on Artificial Intelligence and Statistics*. PMLR; 2023:5714-5730. URL: <https://proceedings.mlr.press/v206/nguyen23e.html> [Accessed 2026-05-07]
376. Bai L, Hu H, Ye Q, Li H, Wang L, Xu J. Membership inference attacks and defenses in federated learning: a survey. *ACM Comput Surv*. Apr 30, 2025;57(4):1-35. [doi: [10.1145/3704633](https://doi.org/10.1145/3704633)]
377. Commey D, Hounsinou SG, Crosby GV. Post-quantum secure blockchain-based federated learning framework for healthcare analytics. *IEEE Netw Lett*. 2025;7(2):126-129. [doi: [10.1109/LNET.2025.3563434](https://doi.org/10.1109/LNET.2025.3563434)]
378. Li S, Ngai ECH, Voigt T. An experimental study of Byzantine-robust aggregation schemes in federated learning. *IEEE Trans Big Data*. 2024;10(6):975-988. [doi: [10.1109/TBDDATA.2023.3237397](https://doi.org/10.1109/TBDDATA.2023.3237397)]
379. Bonawitz K, Ivanov V, Kreuter B, et al. Practical secure aggregation for privacy-preserving machine learning. Presented at: 2017 ACM SIGSAC Conference on Computer and Communications Security; Oct 30 to Nov 3, 2017; Dallas, TX, USA. [doi: [10.1145/3133956.3133982](https://doi.org/10.1145/3133956.3133982)]
380. McMahan HB, Ramage D, Talwar K, Zhang L. Learning differentially private recurrent language models. arXiv. Preprint posted online on Oct 18, 2017. URL: <https://arxiv.org/abs/1710.06963> [Accessed 2026-05-07]
381. Geyer RC, Klein T, Nabi M. Differentially private federated learning: a client level perspective. arXiv. Preprint posted online on Dec 20, 2017. URL: <https://arxiv.org/abs/1712.07557> [Accessed 2026-05-07]
382. Rangwala M, Venugopal KR, Buyya R. Blockchain-enabled federated learning. arXiv. Preprint posted online on Aug 8, 2025. URL: <https://arxiv.org/abs/2508.06406> [Accessed 2026-07-07]
383. Fang F, Feng L, Xie J, et al. BCFL: a trustworthy and efficient federated learning framework based on blockchain in iot. Presented at: 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD); May 8-10, 2024; Tianjin, China. [doi: [10.1109/CSCWD61410.2024.10580415](https://doi.org/10.1109/CSCWD61410.2024.10580415)]
384. Teo ZL, Jin L, Li S, et al. Federated machine learning in healthcare: a systematic review on clinical applications and technical architecture. *Cell Rep Med*. Feb 20, 2024;5(2):101419. [doi: [10.1016/j.xcrm.2024.101419](https://doi.org/10.1016/j.xcrm.2024.101419)] [Medline: [38340728](https://pubmed.ncbi.nlm.nih.gov/38340728/)]
385. Li M, Xu P, Hu J, Tang Z, Yang G. From challenges and pitfalls to recommendations and opportunities: implementing federated learning in healthcare. *Med Image Anal*. Apr 2025;101:103497. [doi: [10.1016/j.media.2025.103497](https://doi.org/10.1016/j.media.2025.103497)] [Medline: [39961211](https://pubmed.ncbi.nlm.nih.gov/39961211/)]

386. Salim MM, Yang LT, Park JH. Privacy-preserving and scalable federated blockchain scheme for healthcare 4.0. *Computer Networks*. Jun 2024;247:110472. [doi: [10.1016/j.comnet.2024.110472](https://doi.org/10.1016/j.comnet.2024.110472)]
387. Moore SK. Chips to compute with encrypted data are coming: fully homomorphic encryption could make data unhackable. *IEEE Spectr*. 2024;61(1):38-40. [doi: [10.1109/MSPEC.2024.10380468](https://doi.org/10.1109/MSPEC.2024.10380468)]
388. Karimireddy SP, He L, Jaggi M. Learning from history for Byzantine robust optimization. In: *Proceedings of the 38th International Conference on Machine Learning*. PMLR; 2021:5311-5319. URL: <https://proceedings.mlr.press/v139/karimireddy21a.html> [Accessed 2026-05-07]
389. Komlo C, Goldberg I. FROST: flexible round-optimized Schnorr threshold signatures. In: Dunkelman O, Jacobson MJ, O'Flynn C, editors. *Selected Areas in Cryptography SAC 2020 Lecture Notes in Computer Science*. Springer; 2021:34-65. [doi: [10.1007/978-3-030-81652-0_2](https://doi.org/10.1007/978-3-030-81652-0_2)]
390. Pati S, Baid U, Edwards B, et al. The federated tumor segmentation (FeTS) tool: an open-source solution to further solid tumor research. *Phys Med Biol*. Oct 12, 2022;67(20):204002. [doi: [10.1088/1361-6560/ac9449](https://doi.org/10.1088/1361-6560/ac9449)] [Medline: [36137534](https://pubmed.ncbi.nlm.nih.gov/36137534/)]
391. The HIPAA privacy rule. US Department of Health and Human Services. URL: <https://www.hhs.gov/hipaa/for-professionals/privacy/index.html> [Accessed 2026-05-07]
392. European Parliament and Council of the European Union. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. *EUR-Lex*. 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [Accessed 2026-05-07]
393. Altameem A, Kovtun V, Al-Ma'aitah M, Altameem T, H F, Youssef AE. Patient's data privacy protection in medical healthcare transmission services using back propagation learning. *Computers and Electrical Engineering*. Sep 2022;102:108087. [doi: [10.1016/j.compeleceng.2022.108087](https://doi.org/10.1016/j.compeleceng.2022.108087)]
394. Artificial intelligence in software as a medical device. US Food and Drug Administration. URL: <https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-software-medical-device> [Accessed 2026-05-07]
395. Sinaci AA, Gencturk M, Alvarez-Romero C, et al. Privacy-preserving federated machine learning on FAIR health data: a real-world application. *Comput Struct Biotechnol J*. Dec 2024;24:136-145. [doi: [10.1016/j.csbj.2024.02.014](https://doi.org/10.1016/j.csbj.2024.02.014)] [Medline: [38434250](https://pubmed.ncbi.nlm.nih.gov/38434250/)]
396. Tölle M, Garthe P, Scherer C, et al. Real world federated learning with a knowledge distilled transformer for cardiac CT imaging. *NPJ Digit Med*. Feb 6, 2025;8(1):88. [doi: [10.1038/s41746-025-01434-3](https://doi.org/10.1038/s41746-025-01434-3)] [Medline: [39915633](https://pubmed.ncbi.nlm.nih.gov/39915633/)]
397. Shick AA, Webber CM, Kiarashi N, et al. Transparency of artificial intelligence/machine learning-enabled medical devices. *NPJ Digit Med*. Jan 26, 2024;7(1):21. [doi: [10.1038/s41746-023-00992-8](https://doi.org/10.1038/s41746-023-00992-8)] [Medline: [38273098](https://pubmed.ncbi.nlm.nih.gov/38273098/)]
398. Leslie K, Moore J, Robertson C, et al. Regulating health professional scopes of practice: comparing institutional arrangements and approaches in the US, Canada, Australia and the UK. *Hum Resour Health*. Jan 28, 2021;19(1):15. [doi: [10.1186/s12960-020-00550-3](https://doi.org/10.1186/s12960-020-00550-3)] [Medline: [33509209](https://pubmed.ncbi.nlm.nih.gov/33509209/)]
399. Tan E, Lerouge E, Du Caju J, Du Seuil D. Verification of education credentials on European blockchain services infrastructure (EBSI): action research in a cross-border use case between Belgium and Italy. *BDCC*. 2023;7(2):79. [doi: [10.3390/bdcc7020079](https://doi.org/10.3390/bdcc7020079)]
400. Orabi MM, Emam O, Fahmy H. Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review. *J Big Data*. 2025;12(1):55. [doi: [10.1186/s40537-025-01099-5](https://doi.org/10.1186/s40537-025-01099-5)]
401. Kalapaaking AP, Khalil I, Yi X, Lam KY, Huang GB, Wang N. Auditable and verifiable federated learning based on blockchain-enabled decentralization. *IEEE Trans Neural Netw Learning Syst*. 2024;36(1):102-115. [doi: [10.1109/TNNLS.2024.3407670](https://doi.org/10.1109/TNNLS.2024.3407670)]
402. Kostick-Quenet KM, Compagnucci MC, Aboy M, Minssen T. Patient-centric federated learning: automating meaningful consent to health data sharing with smart contracts. *J Law Biosci*. 2025;12(1):lsaf003. [doi: [10.1093/jlb/lsaf003](https://doi.org/10.1093/jlb/lsaf003)] [Medline: [40321304](https://pubmed.ncbi.nlm.nih.gov/40321304/)]
403. Siniosoglou I, Argyriou V, Sarigiannidis P, et al. Post-processing fairness evaluation of federated models: an unsupervised approach in healthcare. *IEEE/ACM Trans Comput Biol and Bioinf*. 2023;20(4):2518-2529. [doi: [10.1109/TCBB.2023.3269767](https://doi.org/10.1109/TCBB.2023.3269767)]
404. McKay F, Williams BJ, Prestwich G, Bansal D, Treanor D, Hallowell N. Artificial intelligence and medical research databases: ethical review by data access committees. *BMC Med Ethics*. Jul 8, 2023;24(1):49. [doi: [10.1186/s12910-023-00927-8](https://doi.org/10.1186/s12910-023-00927-8)] [Medline: [37422629](https://pubmed.ncbi.nlm.nih.gov/37422629/)]
405. Zafar A. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. *Journal of Cybersecurity*. Jan 17, 2025;11(1). [doi: [10.1093/cybsec/tyaf002](https://doi.org/10.1093/cybsec/tyaf002)]
406. Belen-Saglam R, Altuncu E, Lu Y, Li S. A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*. Jun 2023;4(2):100129. [doi: [10.1016/j.bcra.2023.100129](https://doi.org/10.1016/j.bcra.2023.100129)]
407. Balistri E, Casellato F, Giannelli C, Stefanelli C. BlockHealth: blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. *ICT Express*. Sep 2021;7(3):308-315. [doi: [10.1016/j.icte.2021.08.006](https://doi.org/10.1016/j.icte.2021.08.006)]
408. Makhdoom I, Zhou I, Abolhasan M, Lipman J, Ni W. PrivySharing: a blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*. Jan 2020;88:101653. [doi: [10.1016/j.cose.2019.101653](https://doi.org/10.1016/j.cose.2019.101653)]

409. Zhang F, Shuai Z, Kuang K, Wu F, Zhuang Y, Xiao J. Unified fair federated learning for digital healthcare. *Patterns* (N Y). Jan 12, 2024;5(1):100907. [doi: [10.1016/j.patter.2023.100907](https://doi.org/10.1016/j.patter.2023.100907)] [Medline: [38264718](https://pubmed.ncbi.nlm.nih.gov/38264718/)]
410. Poulain R, Tarek MFB, Beheshti R. Improving fairness in AI models on electronic health records: the case for federated learning methods. arXiv. Preprint posted online on May 19, 2023. URL: <https://arxiv.org/abs/2305.11386> [Accessed 2026-05-07]
411. Liu M, Ning Y, Teixayavong S, et al. A scoping review and evidence gap analysis of clinical AI fairness. *NPJ Digit Med*. Jun 14, 2025;8(1):360. [doi: [10.1038/s41746-025-01667-2](https://doi.org/10.1038/s41746-025-01667-2)] [Medline: [40517148](https://pubmed.ncbi.nlm.nih.gov/40517148/)]
412. Li S, Wu Q, Zhou D, et al. FairFML: fair federated machine learning with a case study on reducing gender disparities in cardiac arrest outcome prediction. *NPJ Health Syst*. 2025;2(1):29. [doi: [10.1038/s44401-025-00035-2](https://doi.org/10.1038/s44401-025-00035-2)]
413. Xing H, Sun R, Ren J, et al. Achieving flexible fairness metrics in federated medical imaging. *Nat Commun*. Apr 8, 2025;16(1):3342. [doi: [10.1038/s41467-025-58549-0](https://doi.org/10.1038/s41467-025-58549-0)] [Medline: [40199877](https://pubmed.ncbi.nlm.nih.gov/40199877/)]
414. Friesen P, Douglas-Jones R, Marks M, et al. Governing AI-driven health research: are IRBs up to the task? *Ethics & Human Research*. Mar 2021;43(2):35-42. [doi: [10.1002/eahr.500085](https://doi.org/10.1002/eahr.500085)]
415. Capili B, Anastasi JK. Ethical research and the institutional review board: an introduction. *Am J Nurs*. Mar 1, 2024;124(3):50-54. [doi: [10.1097/01.NAJ.0001008420.28033.e8](https://doi.org/10.1097/01.NAJ.0001008420.28033.e8)] [Medline: [38386835](https://pubmed.ncbi.nlm.nih.gov/38386835/)]
416. Boudierhem R. Shaping the future of AI in healthcare through ethics and governance. *Humanit Soc Sci Commun*. 2024;11(1). [doi: [10.1057/s41599-024-02894-w](https://doi.org/10.1057/s41599-024-02894-w)]
417. Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization. 2021. URL: <https://www.who.int/publications/i/item/9789240029200> [Accessed 2026-07-05]
418. Secretary's Advisory Committee on Human Research Protections. IRB considerations on the use of artificial intelligence in human subjects research. US Department of Health and Human Services. 2022. URL: <https://www.hhs.gov/ohrp/sachrp-committee/recommendations/irb-considerations-use-artificial-intelligence-human-subjects-research/index.html> [Accessed 2026-05-07]
419. Kiseleva A, Kotzinos D, De Hert P. Transparency of AI in healthcare as a multilayered system of accountabilities: between legal requirements and technical limitations. *Front Artif Intell*. 2022;5:879603. [doi: [10.3389/frai.2022.879603](https://doi.org/10.3389/frai.2022.879603)] [Medline: [35707765](https://pubmed.ncbi.nlm.nih.gov/35707765/)]
420. Holzinger A, Saranti A, Molnar C, Biecek P, Samek W. Explainable AI methods - a brief overview. In: Holzinger A, Goebel R, Fong R, Moon T, Müller KR, Samek W, editors. *xxAI - Beyond Explainable AI xxAI 2020 Lecture Notes in Computer Science*. Springer; 2022:13-38. [doi: [10.1007/978-3-031-04083-2_2](https://doi.org/10.1007/978-3-031-04083-2_2)]
421. Amann J, Blasimme A, Vayena E, Frey D, Madai VI, Precise4Q Consortium. Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. *BMC Med Inform Decis Mak*. Nov 30, 2020;20(1):310. [doi: [10.1186/s12911-020-01332-6](https://doi.org/10.1186/s12911-020-01332-6)] [Medline: [33256715](https://pubmed.ncbi.nlm.nih.gov/33256715/)]
422. Sadeghi Z, Alizadehsani R, Cifci MA, et al. A review of explainable artificial intelligence in healthcare. *Computers and Electrical Engineering*. Aug 2024;118:109370. [doi: [10.1016/j.compeleceng.2024.109370](https://doi.org/10.1016/j.compeleceng.2024.109370)]
423. Jobin A, Ienca M, Vayena E. The global landscape of AI ethics guidelines. *Nat Mach Intell*. 2019;1(9):389-399. [doi: [10.1038/s42256-019-0088-2](https://doi.org/10.1038/s42256-019-0088-2)]
424. Rauter CM, Wöhlke S, Schicktanz S. My data, my choice? - German patient organizations' attitudes towards big data-driven approaches in personalized medicine. an empirical-ethical study. *J Med Syst*. Feb 22, 2021;45(4):43. [doi: [10.1007/s10916-020-01702-7](https://doi.org/10.1007/s10916-020-01702-7)] [Medline: [33616768](https://pubmed.ncbi.nlm.nih.gov/33616768/)]
425. Shen N, Kassam I, Zhao H, et al. Foundations for meaningful consent in Canada's digital health ecosystem: retrospective study. *JMIR Med Inform*. Mar 31, 2022;10(3):e30986. [doi: [10.2196/30986](https://doi.org/10.2196/30986)] [Medline: [35357318](https://pubmed.ncbi.nlm.nih.gov/35357318/)]
426. Li N, Zhou C, Gao Y, et al. Machine unlearning: taxonomy, metrics, applications, challenges, and prospects. *IEEE Trans Neural Netw Learning Syst*. 2025;36(8):13709-13729. [doi: [10.1109/TNNLS.2025.3530988](https://doi.org/10.1109/TNNLS.2025.3530988)]
427. Liu Z, Jiang Y, Shen J, et al. A survey on federated unlearning: challenges, methods, and future directions. *ACM Comput Surv*. Jan 31, 2025;57(1):1-38. [doi: [10.1145/3679014](https://doi.org/10.1145/3679014)]
428. Bhardwaj T, Sumangali K. An explainable federated blockchain framework with privacy-preserving AI optimization for securing healthcare data. *Sci Rep*. Jul 1, 2025;15(1):21799. [doi: [10.1038/s41598-025-04083-4](https://doi.org/10.1038/s41598-025-04083-4)] [Medline: [40595873](https://pubmed.ncbi.nlm.nih.gov/40595873/)]
429. Blackman J, Veerapen R. On the practical, ethical, and legal necessity of clinical artificial intelligence explainability: an examination of key arguments. *BMC Med Inform Decis Mak*. Mar 5, 2025;25(1):111. [doi: [10.1186/s12911-025-02891-2](https://doi.org/10.1186/s12911-025-02891-2)] [Medline: [40045339](https://pubmed.ncbi.nlm.nih.gov/40045339/)]
430. Artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD) action plan. US Food and Drug Administration. 2021. URL: <https://www.fda.gov/media/145022/download> [Accessed 2026-05-07]
431. Kauttonen J, Rousi R, Alamäki A. Trust and acceptance challenges in the adoption of AI applications in health care: quantitative survey analysis. *J Med Internet Res*. Mar 21, 2025;27:e65567. [doi: [10.2196/65567](https://doi.org/10.2196/65567)] [Medline: [40116853](https://pubmed.ncbi.nlm.nih.gov/40116853/)]
432. Dayan I, Roth HR, Zhong A, et al. Federated learning for predicting clinical outcomes in patients with COVID-19. *Nat Med*. Oct 2021;27(10):1735-1743. [doi: [10.1038/s41591-021-01506-3](https://doi.org/10.1038/s41591-021-01506-3)] [Medline: [34526699](https://pubmed.ncbi.nlm.nih.gov/34526699/)]
433. Kumar R, Khan AA, Kumar J, et al. Blockchain-federated-learning and deep learning models for COVID-19 detection using CT imaging. *IEEE Sensors J*. 2021;21(14):16301-16314. [doi: [10.1109/JSEN.2021.3076767](https://doi.org/10.1109/JSEN.2021.3076767)]

434. Pati S, Baid U, Edwards B, et al. Federated learning enables big data for rare cancer boundary detection. *Nat Commun.* Dec 5, 2022;13(1):7346. [doi: [10.1038/s41467-022-33407-5](https://doi.org/10.1038/s41467-022-33407-5)] [Medline: [36470898](https://pubmed.ncbi.nlm.nih.gov/36470898/)]
435. Zenk M, Baid U, Pati S, et al. Towards fair decentralized benchmarking of healthcare AI algorithms with the federated tumor segmentation (FeTS) challenge. *Nat Commun.* Jul 8, 2025;16(1):6274. [doi: [10.1038/s41467-025-60466-1](https://doi.org/10.1038/s41467-025-60466-1)] [Medline: [40628696](https://pubmed.ncbi.nlm.nih.gov/40628696/)]
436. Mazid A, Kirmani S, Abid M, Pawar V. A secure and efficient framework for internet of medical things through blockchain driven customized federated learning. *Cluster Comput.* Aug 2025;28(4):225. [doi: [10.1007/s10586-024-04896-4](https://doi.org/10.1007/s10586-024-04896-4)]
437. Moulahi W, Jdey I, Moulahi T, Alawida M, Alabdulatif A. A blockchain-based federated learning mechanism for privacy preservation of healthcare IoT data. *Comput Biol Med.* Dec 2023;167:107630. [doi: [10.1016/j.compbimed.2023.107630](https://doi.org/10.1016/j.compbimed.2023.107630)] [Medline: [37952305](https://pubmed.ncbi.nlm.nih.gov/37952305/)]
438. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced Internet of Health Things framework: a blockchain managed federated learning approach. *IEEE Access.* 2020;8:205071-205087. [doi: [10.1109/ACCESS.2020.3037474](https://doi.org/10.1109/ACCESS.2020.3037474)] [Medline: [34192116](https://pubmed.ncbi.nlm.nih.gov/34192116/)]
439. Ahmed AA, Alabi OO. Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: a systematic review. *IEEE Access.* 2024;12:102219-102241. [doi: [10.1109/ACCESS.2024.3429205](https://doi.org/10.1109/ACCESS.2024.3429205)]
440. Petrosino L, Masi L, D'Antoni F, Merone M, Vollero L. A zero-knowledge proof federated learning on DLT for healthcare data. *J Parallel Distrib Comput.* Feb 2025;196:104992. [doi: [10.1016/j.jpdc.2024.104992](https://doi.org/10.1016/j.jpdc.2024.104992)]
441. Jiang Y, Ma B, Wang X, et al. Blockchain federated learning for Internet of Things: a comprehensive survey. *ACM Comput Surv.* Oct 31, 2024;56(10):1-37. [doi: [10.1145/3659099](https://doi.org/10.1145/3659099)]
442. Chang Y, Fang C, Sun W. A blockchain-based federated learning method for smart healthcare. *Comput Intell Neurosci.* 2021;2021(1):4376418. [doi: [10.1155/2021/4376418](https://doi.org/10.1155/2021/4376418)] [Medline: [34868289](https://pubmed.ncbi.nlm.nih.gov/34868289/)]
443. Zhang H, Jiang S, Xuan S. Decentralized federated learning based on blockchain: concepts, framework, and challenges. *Comput Commun.* Feb 2024;216:140-150. [doi: [10.1016/j.comcom.2023.12.042](https://doi.org/10.1016/j.comcom.2023.12.042)]
444. Samantray BS, Reddy KHK. A federated learning approach towards hybrid blockchain, quantum-key-encryption based distributed system: a futuristic healthcare architecture for smart cities. *Blockchain: Research and Applications.* Sep 2025;100385:100385. [doi: [10.1016/j.bcra.2025.100385](https://doi.org/10.1016/j.bcra.2025.100385)]
445. Bhasker B, Rao PM, Saraswathi P, et al. Blockchain framework with IoT device using federated learning for sustainable healthcare systems. *Sci Rep.* Jul 23, 2025;15(1):26736. [doi: [10.1038/s41598-025-06539-z](https://doi.org/10.1038/s41598-025-06539-z)] [Medline: [40701986](https://pubmed.ncbi.nlm.nih.gov/40701986/)]
446. Ali AA, Gunavathie MA, Srinivasan V, Aruna M, Chennappan R, Matheena M. Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare. *Clinical eHealth.* Dec 2025;8:125-133. [doi: [10.1016/j.ceh.2025.04.002](https://doi.org/10.1016/j.ceh.2025.04.002)]
447. Das P, Kumar N, Jain C, Singh M. Intelligent IoT-enabled healthcare solutions implementing federated meta-learning with blockchain. *J Ind Inf Integr.* May 2025;45:100797. [doi: [10.1016/j.jii.2025.100797](https://doi.org/10.1016/j.jii.2025.100797)]
448. Kumar R, Bernard CM, Ullah A, et al. Privacy-preserving blockchain-based federated learning for brain tumor segmentation. *Comput Biol Med.* Jul 2024;177:108646. [doi: [10.1016/j.compbimed.2024.108646](https://doi.org/10.1016/j.compbimed.2024.108646)] [Medline: [38824788](https://pubmed.ncbi.nlm.nih.gov/38824788/)]
449. Liang X, Zhao J, Chen Y, Bandara E, Shetty S. Architectural design of a blockchain-enabled, federated learning platform for algorithmic fairness in predictive health care: design science study. *J Med Internet Res.* Oct 30, 2023;25:e46547. [doi: [10.2196/46547](https://doi.org/10.2196/46547)] [Medline: [37902833](https://pubmed.ncbi.nlm.nih.gov/37902833/)]
450. Om Kumar CU, Gajendran S, Balaji V, Nhaveen A, Sai Balakrishnan S. RETRACTED ARTICLE: Securing health care data through blockchain enabled collaborative machine learning. *Soft comput.* 2023;27(14):9941-9954. [doi: [10.1007/s00500-023-08330-6](https://doi.org/10.1007/s00500-023-08330-6)] [Medline: [37287568](https://pubmed.ncbi.nlm.nih.gov/37287568/)]
451. Ali A, Al-Rimy BAS, Tin TT, Altamimi SN, Qasem SN, Saeed F. Empowering precision medicine: unlocking revolutionary insights through blockchain-enabled federated learning and electronic medical records. *Sensors (Basel).* Aug 28, 2023;23(17):7476. [doi: [10.3390/s23177476](https://doi.org/10.3390/s23177476)] [Medline: [37687931](https://pubmed.ncbi.nlm.nih.gov/37687931/)]
452. Lian Z, Wang W, Han Z, Su C. Blockchain-based personalized federated learning for Internet of Medical Things. *IEEE Trans Sustain Comput.* 2023;8(4):694-702. [doi: [10.1109/TSUSC.2023.3279111](https://doi.org/10.1109/TSUSC.2023.3279111)]
453. Farooq K, Syed HJ, Alqahtani SO, Nagmeldin W, Ibrahim AO, Gani A. Blockchain federated learning for in-home health monitoring. *Electronics (Basel).* 2022;12(1):136. [doi: [10.3390/electronics12010136](https://doi.org/10.3390/electronics12010136)]
454. Zhang H, Li G, Zhang Y, Gai K, Qiu M. Blockchain-based privacy-preserving medical data sharing scheme using federated learning. In: Qiu H, Zhang C, Fei Z, Qiu M, Kung SY, editors. *Knowledge Science, Engineering and Management KSEM 2021 Lecture Notes in Computer Science.* Springer; 2021:634-646. [doi: [10.1007/978-3-030-82153-1_52](https://doi.org/10.1007/978-3-030-82153-1_52)]
455. Lo SK, Liu Y, Lu Q, et al. Toward trustworthy AI: blockchain-based architecture design for accountability and fairness of federated learning systems. *IEEE Internet Things J.* 2022;10(4):3276-3284. [doi: [10.1109/JIOT.2022.3144450](https://doi.org/10.1109/JIOT.2022.3144450)]
456. Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B. A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology. *Future Generation Computer Systems.* Apr 2022;129:380-388. [doi: [10.1016/j.future.2021.11.028](https://doi.org/10.1016/j.future.2021.11.028)]

457. Nguyen DC, Ding M, Pham QV, et al. Federated learning meets blockchain in edge computing: opportunities and challenges. *IEEE Internet Things J.* 2021;8(16):12806-12825. [doi: [10.1109/JIOT.2021.3072611](https://doi.org/10.1109/JIOT.2021.3072611)]
458. Liu Y, Yu W, Ai Z, Xu G, Zhao L, Tian Z. A blockchain-empowered federated learning in healthcare-based cyber physical systems. *IEEE Trans Netw Sci Eng.* 2022;10(5):2685-2696. [doi: [10.1109/TNSE.2022.3168025](https://doi.org/10.1109/TNSE.2022.3168025)]
459. Otoum S, Al Ridhawi I, Mouftah HT. Preventing and controlling epidemics through blockchain-assisted AI-enabled networks. *IEEE Netw.* 2021;35(3):34-41. [doi: [10.1109/MNET.011.2000628](https://doi.org/10.1109/MNET.011.2000628)]
460. Durga R, Poovammal E. Federated learning model for healthchain system. Presented at: 2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE); Dec 1-3, 2021; Kedah, Malaysia. [doi: [10.1109/ICRAIE52900.2021.9703948](https://doi.org/10.1109/ICRAIE52900.2021.9703948)]
461. Lakhan A, Mohammed MA, Nedoma J, et al. Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare. *IEEE J Biomed Health Inform.* 2022;27(2):664-672. [doi: [10.1109/JBHI.2022.3165945](https://doi.org/10.1109/JBHI.2022.3165945)]
462. Samuel O, Omojo AB, Onuja AM, et al. IoMT: a COVID-19 healthcare system driven by federated learning and blockchain. *IEEE J Biomed Health Inform.* 2022;27(2):823-834. [doi: [10.1109/JBHI.2022.3143576](https://doi.org/10.1109/JBHI.2022.3143576)]
463. Yang X, Xing C. Federated medical learning framework based on blockchain and homomorphic encryption. *Wireless Communications and Mobile Computing.* Jan 5, 2024;2024:1-15. [doi: [10.1155/2024/8138644](https://doi.org/10.1155/2024/8138644)]
464. Nguyen DC, Ding M, Pathirana PN, Seneviratne A. Blockchain and AI-based solutions to combat coronavirus (COVID-19)-like epidemics: a survey. *IEEE Access.* 2021;9:95730-95753. [doi: [10.1109/ACCESS.2021.3093633](https://doi.org/10.1109/ACCESS.2021.3093633)] [Medline: [34812398](https://pubmed.ncbi.nlm.nih.gov/34812398/)]
465. Hemdan EED, Sayed A. Smart and secure healthcare with digital twins: a deep dive into blockchain, federated learning, and future innovations. *Algorithms.* 2025;18(7):401. [doi: [10.3390/a18070401](https://doi.org/10.3390/a18070401)]
466. Baseri Y, Hafid A, Shahsavari Y, Makrakis D, Khodaiemehr H. Blockchain security risk assessment in quantum era, migration strategies, and proactive defense. *IEEE Commun Surv Tutor.* 2025;28:2925-2964. [doi: [10.1109/COMST.2025.3621113](https://doi.org/10.1109/COMST.2025.3621113)]
467. Cheon JH, Kim A, Kim M, Song Y. Homomorphic encryption for arithmetic of approximate numbers. In: Takagi T, Peyrin T, editors. *Advances in Cryptology – ASIACRYPT 2017 ASIACRYPT 2017 Lecture Notes in Computer Science.* Springer; 2017:409-437. [doi: [10.1007/978-3-319-70694-8_15](https://doi.org/10.1007/978-3-319-70694-8_15)]
468. Doga H, Bose A, Sahin ME, et al. How can quantum computing be applied in clinical trial design and optimization? *Trends Pharmacol Sci.* Oct 2024;45(10):880-891. [doi: [10.1016/j.tips.2024.08.005](https://doi.org/10.1016/j.tips.2024.08.005)] [Medline: [39317621](https://pubmed.ncbi.nlm.nih.gov/39317621/)]
469. Thibault LT, Sarry T, Hafid AS. Blockchain scaling using rollups: a comprehensive survey. *IEEE Access.* 2022;10:93039-93054. [doi: [10.1109/ACCESS.2022.3200051](https://doi.org/10.1109/ACCESS.2022.3200051)]
470. Hafid A, Hafid AS, Samih M. Scaling blockchains: a comprehensive survey. *IEEE Access.* 2020;8:125244-125262. [doi: [10.1109/ACCESS.2020.3007251](https://doi.org/10.1109/ACCESS.2020.3007251)]
471. You J, Yang R, Zhan Y, Song B, Zhang Y, Wang Z. BR-MTFL: a novel Byzantine resilience-enhanced multitask federated learning framework for high-speed train fault diagnosis. *IEEE Trans Instrum Meas.* 2025;74:1-13. [doi: [10.1109/TIM.2025.3550635](https://doi.org/10.1109/TIM.2025.3550635)]
472. Yang N, Tang C, Deng Z, He D. A Gaussian reputation-based hybrid BFT consensus with a formal security framework. *IEEE Trans Dependable and Secure Comput.* 2025;22(5):5397-5414. [doi: [10.1109/TDSC.2025.3567356](https://doi.org/10.1109/TDSC.2025.3567356)]
473. Wang Y, Peng H, Su Z, Luan TH, Benslimane A, Wu Y. A platform-free proof of federated learning consensus mechanism for sustainable blockchains. *IEEE J Select Areas Commun.* 2022;40(12):3305-3324. [doi: [10.1109/JSAC.2022.3213347](https://doi.org/10.1109/JSAC.2022.3213347)]
474. Ajmal CS, Yerram S, Abishek V, et al. Innovative approaches in regulatory affairs: leveraging artificial intelligence and machine learning for efficient compliance and decision-making. *AAPS J.* Jan 7, 2025;27(1):22. [doi: [10.1208/s12248-024-01006-5](https://doi.org/10.1208/s12248-024-01006-5)] [Medline: [39776314](https://pubmed.ncbi.nlm.nih.gov/39776314/)]
475. Dubey P, Kumar M. Integrating explainable AI with federated learning for next-generation IoT: a comprehensive review and prospective insights. *Computer Science Review.* May 2025;56:100697. [doi: [10.1016/j.cosrev.2024.100697](https://doi.org/10.1016/j.cosrev.2024.100697)]
476. Smith V, Chiang CK, Sanjabi M, Talwalkar A. Federated multi-task learning. Presented at: 31st International Conference on Neural Information Processing Systems; Dec 4-9, 2017; Long Beach, CA, USA. [doi: [10.5555/3294996.3295196](https://doi.org/10.5555/3294996.3295196)]
477. Li K, Xiao C. CBFL: a communication-efficient federated learning framework from data redundancy perspective. *IEEE Systems Journal.* ;16(4):5572-5583. [doi: [10.1109/JSYST.2021.3119152](https://doi.org/10.1109/JSYST.2021.3119152)]

Abbreviations

- AI:** artificial intelligence
BCFL: blockchain-based federated learning
BFT: Byzantine fault tolerance
CT: computed tomography
DAG: direct acyclic graph tangle
DApps: decentralized applications

DICOM: Digital Imaging and Communications in Medicine
DP: differential privacy
DPoS: delegated proof of stake
ECG: electrocardiography
EEG: electroencephalography
EHR: electronic health record
FDA: Food and Drug Administration
FL: federated learning
FTL: federated transfer learning
GDPR: General Data Protection Regulation
HE: homomorphic encryption
HFL: horizontal federated learning
HIPAA: Health Insurance Portability and Accountability Act
IBC: Inter-Blockchain Communication
IoMT: Internet of Medical Things
IoT: Internet of Things
MAR: medication administration record
ML: machine learning
MRI: magnetic resonance imaging
NLP: natural language processing
P2P: peer-to-peer
pBFT: practical Byzantine fault tolerance
PGD: patient-generated data
PoA: proof of authority
PoS: proof of stake
PoW: proof of work
PRO: patient-reported outcomes
RL: reinforcement learning
SHAP: Shapley Additive Explanations
SMPC: secure multiparty computation
VFL: vertical federated learning
ZKP: zero-knowledge proof

Edited by Andrew Coristine; peer-reviewed by Nirajan Acharya, Odumbo Oluwole, Oluwafemi Oloruntoba; submitted 05.Jul.2025; final revised version received 18.Jan.2026; accepted 20.Jan.2026; published 15.Jun.2026

Please cite as:

Shahsavari Y, Baseri Y, Hafid A, Dambri OA, Makrakis D

Integration of Federated Learning and Blockchain in Health Care: Tutorial on Medical Data, Architectures, Privacy, Security, and Regulatory Compliance

J Med Internet Res 2026;28:e80178

URL: <https://www.jmir.org/2026/1/e80178>

doi: [10.2196/80178](https://doi.org/10.2196/80178)

© Yahya Shahsavari, Yaser Baseri, Abdelhakim Hafid, Oussama Abderrahmane Dambri, Dimitrios Makrakis. Originally published in the Journal of Medical Internet Research (<https://www.jmir.org>), 15.Jun.2026. This is an open-access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work, first published in the Journal of Medical Internet Research (ISSN 1438-8871), is properly cited. The complete bibliographic information, a link to the original publication on <https://www.jmir.org/>, as well as this copyright and license information must be included.