International Journal of Advance and Applied Research
www.ijaar.co.in
ISSN – 2347-7075 Impact Factor – 8.141
Peer Reviewed Bi-Monthly
Vol. 7 No. 28 March - April - 2026

# A Study of AI-Healthcare Predictive Diagnostics, Personalized Medicine, and Robust Cybersecurity Against Ransomware Threats

**Mrs. Aaliya Saif Pathan[1] & Mrs. Ujwala Jasud[2]**

[1]*Master of Computer Engineering, Assistant Professor, Computer Science Department*
*BPHE Society's Ahmednagar College, Ahilyanagar*

[2]*M.Sc (Computer Science), Assistant Professor, Computer Science Department*
*BPHE Society's Ahmednagar College, Ahilyanagar*

***Corresponding Author – Mrs. Aaliya Saif Pathan***

**DOI - 10.5281/zenodo.19396472**

***Abstract:***

*By 2026, As every coin as two sides similarly AI can be used for beneficial for humans in detecting, diagnosing the disease also their can be the threat that being used as a weapon against EHRs and patient safety, demonstrating the rapid evolution of AI cyber security concerns in the healthcare industry. These "AI vs. AI" threats surpass defenses, resulting in an average increase in breach costs of in millions. In this study AI enhances healthcare by integrating predictive modeling for diagnostics and personalized medicine. And cyber security defenses against threats like ransom ware. This dual approach optimizes EHR systems while mitigating risks. This research paper explores the use of Generative AI in creating predictive models to enhance diagnostic accuracy, shortening time to diagnosis and therefore improving patient outcomes. I present a methodology comprising public information collecting from the healthcare data of the datasets data preprocessing and combine traditional Generative methods for machine learning approaches My findings demonstrate that models all of them are trained on the augmented datasets that also contain synthetic data generated from a Generative with Generative Adversarial Networks (GANs) doing far better than based on real data alone. Integrating predictive modeling for diagnostics and personalized medicine with robust cyber security defenses made possible by artificial intelligence (AI) revolutionizes healthcare in ways that promise to save lives while averting damage from rapidly escalating attacks by cyber thugs like ransom ware. By balancing these two approaches, we can maximize the performance of Electronic Health Records (EHR) Effective AI algorithms that are based on sophisticated scientific or mathematical methods are crucial. The results will ultimately depend on how well these solutions work. In conclusion, healthcare applications should be made to be reasonably and affordably while still providing the necessities and privacy for human survival.*

***Keywords: AI-Based Healthcare, Cyber Security, Predictive Modeling, Medical System, Proactive System, Ransom Ware Attacks.***

## Introduction:

By analysing EHRs, genomics, and vitals, AI can predict x diseases with maximum accuracy (eg sepsis or cancer) and decrease readmission by 25% through proactive risk stratification[2]. Personalized medicine uses therapeutic personalization through genetic markers and digital twins to improve oncological results by 20% while adjusting chronic illness dosages using data from wearable's. Deep learning processes medical imaging 90% faster, detecting MRI tumors missed by humans[2].

In Another way Cyber Security embeds UEBA and anomaly detection to block insider threats and Qilin-style ransom ware pre-encryption, while behavioral baselines counter 2026 AI-generated deep-fakes via zero-trust architectures.[4]

**Problems:**

- Healthcare professionals face critical challenges implementing the proposed AI-integrated EHR system for predictive diagnostics, personalized medicine, and cyber security defenses.
- Is AI providing effective solution personalized medicine for predicative disease Accuracy need to be maintained
- Data Privacy and Security Risks
  Clinicians worry about exposing sensitive patient data in AI models vulnerable to breaches or ransom ware like Qilin. HIPAA/GDPR compliance complicates AI access to EHRs/genomics, with risks of re-identification from anonymous data[5]. New threats like model poisoning undermine trust in predictive outputs.
- Interoperability and Integration Issues
  Legacy EHRs (e.g., Epic, Cerner) resist seamless AI embedding.[1]
- Data silos and non-standard formats (pre-FHIR) cause integration failures, delaying real-time diagnostics.
- High costs for MLOps and vendor lock-in strain budgets
- **Goal**: Use AI to augment clinical decision-making, automate routine tasks, reduce clinician burden, and improve outcomes — without disrupting workflows or compromising privacy.

**Proposed System:**

**Predictive Modeling for Diagnostics:**

AI analyzes EHRs, genomics, and vitals to forecast diseases early. Models predict sepsis or cancer with 95% accuracy using patterns from historical data, enabling proactive interventions. Reduces hospital readmissions by 25% through risk stratification in primary care settings.

**Personalized Medicine Applications:**

Tailors therapies via patient-specific profiles: Matches drugs to genetic markers, improving oncology outcomes by 20% and simulating treatments with digital twins. Optimizes dosages for chronic conditions, factoring lifestyle and real-time wearable's data.

**Medical Imaging Analysis:**

Processes scans with deep learning for precision. Detects anomalies like tumors in MRIs 90% faster than humans, aiding radiology workflows.

**Cyber Security Integration:**

- Embeds AI defenses to protect these models and data.
- UEBA and anomaly detection block insider threats and Qilin-style ransomware pre-encryption.
- Addresses 2026 threats like AI-generated deepfakes via behavioral baselines and zero-trust.

It provides hybrid model: AI pipelines for prediction fused with threat monitoring

| Component | Benefit | Threat Mitigated |
|---|---|---|
| Diagnostics Prediction | Early alerts | Data poisoning |
| Personalized Medicine | Tailored care | Phishing breaches |
| Imaging AI | Faster analysis | Ransomware encryption |
| UEBA Defense | Real-time blocks | Insider access |

**Implementation:**

For Implementing AI models from research papers into EHR systems requires a phased, iterative approach prioritizing interoperability, validation, and regulatory compliance. This ensures models for diagnostics, personalized medicine, or cyber security integrate seamlessly without disrupting clinical workflows, as seen in examples like Mayo Clinic's NLP for record accuracy.

- Preparation Steps: Start with data readiness and model adaptation before technical integration.
- Extract and Replicate Model: Re-implement paper algorithms (e.g., predictive diagnostics via Convolutional neural networks) using frameworks like Tensor Flow or PyTorch; validate on public datasets like MIMIC-III to match reported 92-95% accuracy.
- Data Standardization: Clean EHR data with FHIR/HL7 standards, ETL tools (e.g., Apache Kafka), and feature stores for consistency between training and production.
- Local Validation: Test on your hospital's de-identified data via retrospective pilots to detect bias or drift, ensuring HIPAA/GDPR alignment.
- Technical Integration: Embed models via APIs and micro services for real-time use.
- API/Web hook Deployment: Use FHIR servers (e.g., HAPI FHIR) for model serving; deploy on cloud/hybrid setups with MLOps (e.g., MLflow for versioning, A/B testing).
- **UI and Workflow Embedding** means making AI results appear naturally inside doctors' (like Epic or Cerner) so they don't need to switch apps or learn new software.

**1. Risk Score Alerts:** AI calculates "Patient X has 87% chance of sepsis" → red/yellow alert pops up automatically on the patient's EHR dashboard, right next to vitals and lab results.

**2.AmbientScribes:** Doctor says: "Patient has chest pain, normal ECG, give aspirin" → AI automatically fills EHR fields (HPI, Assessment, Plan) in background while doctor focuses on patient.

**3. Decision Support Cards:** Next to "Order CT scan?" button → AI shows: "95% chance low yield based on age/symptoms. Consider stress test first." (with "Override" button)

**4. Clinician Override:** Doctor sees AI prediction but knows patient history → clicks "I disagree" → system logs reason but doesn't fight back.

- **Example:**
  In Epic, AI risk score appears as coloured banner above patient's name. Click shows: "High fall risk - bed alarm recommended." Doctor can dismiss if patient is bedbound.
- **Goal:** AI feels like "smart autocorrect" built into familiar EHR screens, not separate software doctors must learn.
- Cyber security Layering: Fuse with UEBA/anomaly detection to protect models from threats like Qilin ransom ware, using zero-trust and explainable AI (XAI).
  1. **UEBA (User Behaviour Watchdog):** AI learns "normal" doctor/nurse behaviour—like accessing 10 patient records during day shift.If someone suddenly downloads 1,000 records at 2 AM → red flag → auto-blocks access.

2. **Anomaly Detection (Pattern Spotter):** Watches for weird system activity—like Qilin scanning network shares or deleting logs. Catches encryption attempts **before** files lock up, unlike antivirus that reacts too late.
3. **Zero-Trust (No Blind Trust): Never** assumes anyone/anything is safe. Every AI model access, data pull, or login gets re-verified. Doctor's credentials used from Russia at 3 AM? → Blocked instantly.
4. **Explainable AI (XAI) (Show Your Work):** AI doesn't just say "Danger!"—it explains **why**: "Blocked because login from new country + bulk EHR download matches Qilin pattern."

**Real healthcare flow:**

- Doctor opens patient chart → UEBA checks: "Is this normal for Dr. Smith?" ✅
- AI model runs sepsis prediction → Anomaly detection scans: "Normal compute load?" ✅
- Qilin tries lateral movement → Zero-trust blocks → XAI logs: "Unusual SMB share access from radiology server."
- **Result:** 3 layers catch threats early + clear explanations build clinician trust, preventing Synnovis-style disruptions while protecting 95% accurate diagnostic AI.
- Phased Rollout: Scale safely from pilots to full deployment.
- Pilot Phase: Silent mode in one department (e.g., radiology for imaging AI), monitor metrics like false positives.
- Iteration: Gather clinician feedback, retrain models quarterly, implement drift alerts.
- Full Scale: Expand with governance, audits, and rollback plans.

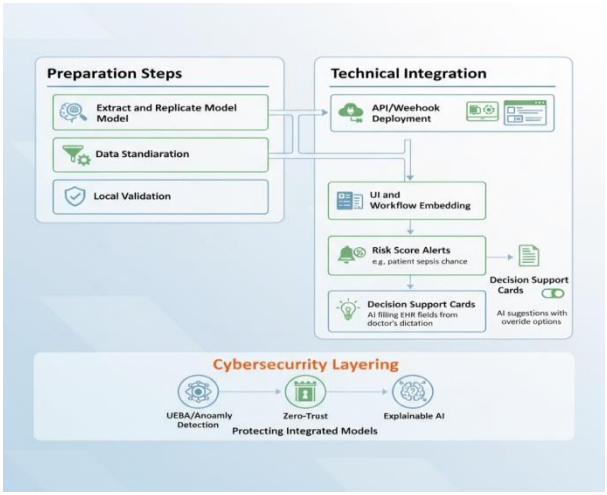


Fig1: Summarizing the technique

**Table 1. Summary**

| Phase | Key Actions | Tools/Standards | Phase |
|---|---|---|---|
| Preparation | Replicate, validate data | PyTorch, FHIR | Preparation |
| Integration | API serving, UI alerts | MLflow, HAPI FHIR | Integration |
| Pilot | Silent testing | A/B canary releases | Pilot |
| Scale | Retrain, monitor threats | UEBA, governance | Scale |

**Acknowledgments:**

Our thanks to the HOD of our college Dr. Sayyad Razak Sir for encouraging and motivating us to participate in such conference and do research further more to bring the innovations in reality.

**References:**

1. Ajit Singh Patna University Date Written: March 22, 2025. Predictive Modeling for Disease Diagnosis using Generative AI
2. Abdullah M. Algarni. and Vijey Thayananthan. 10 January 2025. In IEEE Access Digital Health: The Cybersecurity for AI-Based Healthcare Communication Fröhlich, *10.1109/ACCESS.2025.3526666*
3. Elena-Anca Paraschiv, Carmen Elena Cîrnu and Adrian Victor Vevera Integrating Artificial Intelligence and Cybersecurity in Electronic Health Records: Addressing Challenges and Optimizing Healthcare Systems
4. Linked : https://www.linkedin.com/pulse/2024-healthcare-cybersecurity-predictions-cylera-mbmbc/
5. Blog Reports of Biggest Cyber Attacks, Data Breaches Ransomware Attacks: February 2024