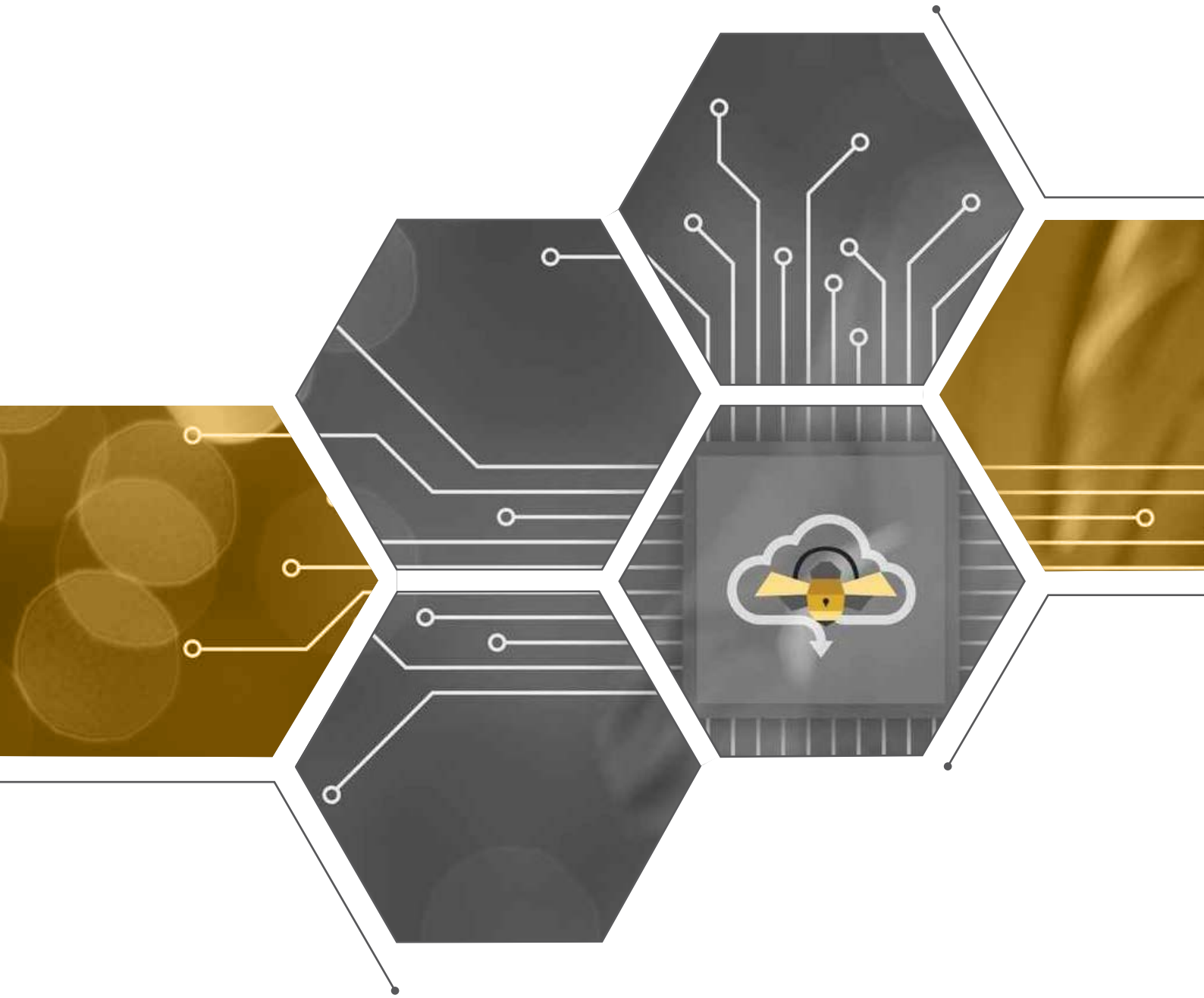
BeeKeeperAI™

Microsoft



Realizing the full potential of healthcare AI

Why confidential computing is the key to driving the industry forward

Healthcare AI: On the precipice of transformed patient care

From harnessing data to develop new treatments to enhancing precision of treatment in ways that make healthcare more effective, equitable—and optimized for each patient—healthcare AI has the potential to transform patient care. Yet to actualize the full potential of healthcare AI, the algorithms used to create healthcare models need to be developed and validated on all the variables they'll face in the real-world clinical setting to ensure consistent performance across clinical environments, patient variables, equipment type, and the clinical workflow. That is, healthcare algorithms must be generalizable in such a way that they are able to perform reliably, regardless of where they're deployed.

To achieve this generalizability, algorithm developers must compute on sufficient amounts of data and protected health information (PHI). However, due to privacy and security concerns, access to PHI has not typically been granted to developers outside of clinical trials. In the instances it can be made available, protecting the algorithm intellectual property (IP) at all times is critical including while it computes on PHI data. Because there hasn't been a secure technical environment for the development of these algorithms, healthcare AI progress has been less than optimal. Until now.

Let's take a look at how confidential computing is accelerating the pace of generalizable healthcare AI by resolving the data sovereignty, privacy, and security issues faced in developing healthcare algorithm models, and by protecting the models' IP—even while in the process of computing on real-world data.

By 2023, 20% of all patient interactions will involve some form of AI enablement within clinical or nonclinical processes, up from less than 4% in 2019.[1]

[1] Gartner, "6 Critical Technologies to Advance Healthcare Ecosystem Orchestration Ability," September 13, 2019.

Defining confidential computing—and why it's the key to accelerating healthcare AI

Confidential computing is a technology capability that protects data and algorithms while at rest (for example, encryption), in transit (for example, Transport Layer Security), and while in use—when they are at their most vulnerable. Computations occur in an attested, hardware-based Trusted Execution Environment (TEE). Algorithms may operate in a variety of confidential computing packages within this TEE, ranging from application "enclaves" that are secured portions of the hardware's processor and memory to full confidential virtual machines (VMs) that are protected from the hypervisor and host operating system.

Using CPU isolation and full memory encryption, confidential computing ensures that data can only be accessed and used by the algorithm or analytic model with specific, granted-access permission. Thus, confidential computing provides a fully isolated and protected zero-trust computation environment for data stewards and algorithm developers. The security features also enable protected AI algorithms to sightlessly compute on protected PHI without compromising intellectual property, patient privacy, or data security.

Because of this ability to enable a zero-trust environment that protects both data and the algorithm IP, confidential computing is the key to accelerating AI innovation and improving outcomes in healthcare around the world.

The United States Presidential Executive Order on Improving the Nation's Cybersecurity (issued May 12, 2021), mandated zero-trust architectures. Confidential computing enables such zero-trust environments with its end-to-end encryption, and enables sightless computing on PHI.

Security stack-up: Where unsecured federated learning falls short

Federated learning (FL) is also a valuable framework for healthcare AI algorithm development. It enables the development of AI models across distributed datasets from multiple organizations alongside the aggregation of machine learning model parameters trained on that distributed data.

But while federated learning does have elements to aid in developing healthcare AI algorithms, it varies from zero-trust in a few key ways:

- No current commercial FL solution is zero-trust.
- Typically, the data steward computational environment is not attested; there are no affirmative means to ensure the algorithm is not a nefarious model.
- The data is also typically exposed during the computation process, allowing an algorithm developer to exfiltrate the data or plant a virus within the data.
- The algorithm parameters are typically transported to the aggregation site in an unsecured manner, exposing both the algorithm IP and potentially the outlier data embedded in the algorithm.
- The aggregation process typically occurs in the clear, allowing for inspection of the variances between site models that often result in a breach of the data or IP.
- The final model is typically not secured or encrypted, leaving it at further risk of exfiltration.

EscrowAI: The only zero-trust collaboration platform leveraging confidential computing

AI development and deployment is automated via the facilitation of collaboration between an algorithm owner and data steward — within EscrowAI's zero-trust environment. See how it works.

Algorithm Owner

Submits a Project Opportunity (POS).

Submits their encrypted algorithm once the data attestation is received, and the algorithm is encapsulated automatically for its journey to the data stewards environment.

Requests a computing run and an attested TEE is created in their Azure environment.

Data Steward

Approves participation in the project.

Curates the data and attests it meets the algorithm developer's specifications.

Encrypts the data & places it within their Azure HIPAA-compliant environment.

Moves the encrypted data inside the TEE by creating a shared access signature (SAS) URL.

Accepts Computing Run.

The algorithm sightlessly processes the data to produce the AI inference once the encrypted data from the SAS URL and the algorithm container are brought into the isolated enclave environment.

During the computing process, the data and algorithm IP are inaccessible. Both the algorithm and dataset are decrypted within the enclave but remain isolated in an encrypted memory space — preventing exposure of any contents to the algorithm owner, to the data steward—or to BeeKeeperAI.

A confidential report is generated in the enclave, validated by EscrowAI, and sent to the algorithm developer's project space, the TEE is decommissioned, and both the data and algorithm are destroyed.

Fully Compliant Zero-Trust Solution

- Project artifacts and computation records are maintained (including data and algorithm versions by computing run) within EscrowAI in a confidential ledger supporting compliance or regulatory requirements.
- Deployment of the TEE and all data and computation activities occur entirely within the Data Steward's HIPAA-compliant Azure environment addressing data sovereignty, privacy, security, and IP protections.

EscrowAI: The only zero-trust collaboration platform leveraging confidential computing

EscrowAI's data privacy, security, and sovereignty features provide:

- **A quadruple security win:** Resolves data sovereignty, privacy, and security as well as protects IP, addressing multiple organizational risks.
- **Increased efficiency and speed to market:** Up to a 90% reduction in contracting and approvals process, which typically requires 12 to 18 months.
- **Computing on real-world PHI:** Enables computing on historically inaccessible data, which promises to enable breakthrough innovations, remove bias, and improve accuracy.
- **Zero-trust architecture:** Leverages secure enclave technology to eliminate the risk of data exfiltration and any interrogation of the algorithm IP during computing.
- **Secure collaboration:** Allows multiple parties to work together securely and collaboratively via user-centric software as a service (SaaS).
- **Permissible use of protected information:** Enables the use of information protected under HIPPA, GDPR, and other privacy regulations for research or healthcare operations activity.
- **IP protection:** Ensures the algorithm is never seen nor shared, even at the host level—for full IP protection.
- **Push-button confidential computing capabilities:** Allows data steward and algorithm developers to take advantage of the power of confidential computing without the need to understand its technical complexities—a single-button push is all it takes.
- **Nonclinical revenue generation:** Enables data stewards to ethically monetize their data for the purposes of advancing innovation in healthcare, from industry-sponsored research agreements, to modern research infrastructure for grants requiring data access, to simplifying data-use agreements and testing commercial AI solutions prior to licensing.

Generalizable AI algorithms can take from 18 to 36 months and cost $2 million to $5 million to achieve the generalizability standard for a single algorithm, making it imperative to protect the IP of the algorithm at all times.[2]

[2] BeeKeeperAI.com

EscrowAI and Azure confidential computing: Enabling the future of healthcare AI

EscrowAI is backed by the reliability and security of Azure confidential computing, which eliminates the single largest barrier of encryption beyond that for data at-rest and in-transit: data encryption while in use.

With EscrowAI and Azure confidential computing, data encryption and algorithm IP protections resolve data privacy, security, and IP protection concerns now. Deployment and operation of confidential computing in the data steward's regulation-compliant Azure environment enable data sovereignty, ensuring data always remains in the control of the data steward. A comprehensive security architecture dramatically reduces the risk of sensitive data breaches across all parties, including cloud operators, cloud tenants, and the customer's own system administrators, further enhancing privacy and security.

Together, EscrowAI's SaaS solution alongside the deployment of confidential computing workflow—in hours, not days—facilitates nonclinical revenue while minimizing the burden for IT organizations. EscrowAI automatically spins up and down the confidential computing enclave, minimizing the computing costs for data stewards.

Accelerate your healthcare-AI success

Today's evolving healthcare landscape demands greater access to private data and the secure, zero-trust environment to leverage it. EscrowAI from BeeKeeperAI brings secure collaboration, HIPPA-permissible activities, and IP protection to meet this demand, sightlessly and securely.

Find out how your organization can tap into the zero-trust environment of EscrowAI to enable data sovereignty, drive new revenue, and accelerate the future of healthcare AI.

www.beekeeperai.com/contact

Learn more