Solution Brief

Intel Security

BeeKeeperAI™

Confidential Computing Platform Helps Accelerate Healthcare AI from Concept to the Clinic

Removing the barriers to medical data access

BeeKeeperAI™ is a zero trust, privacy–preserving, confidential compute platform that enables secure collaborations between healthcare algorithm developers and health information data stewards, accelerating the development, deployment, and monitoring of artificial intelligence (AI) in healthcare. The platform uses Intel® Software Guard Extensions (Intel® SGX) hardware-based memory encryption to create an enclave where algorithms can run on data with confidentiality.

BeeKeeperAI™

Cyberattacks in healthcare are evolving, becoming more sophisticated and more frequent. Since 2019 in the United States, nearly 120 million healthcare data records have been breached. (Alder S, 2022). In 2021, the average total cost of a data breach in healthcare was $9.42 million, a $2 million increase over 2020. At an average per record cost of $161, healthcare data breaches may cost as much as $19 billion. (IBM, 2021) While digitization and technology have brought huge benefits, they have also introduced the loss of confidential data. Whether it is caused by malicious attack or accidental mistake, the consequences are potentially devastating.

With so much at stake, stewards of Protected Health Information (i.e., data stewards) are increasing the protections around that data. It is no longer sufficient to rely on contractual terms or historical relationships as the basis for trust. Increased data security requirements are inhibiting the ability of healthcare provider organizations to deliver digital innovation, including healthcare artificial intelligence, that relies on data access for development, validation, and regulatory approval.

Fortunately, confidential computing and privacy-preserving analytic technologies have demonstrated their capability to protect highly sensitive, regulated data within the financial and government security sectors. BeeKeeperAI now applies these technologies to healthcare.

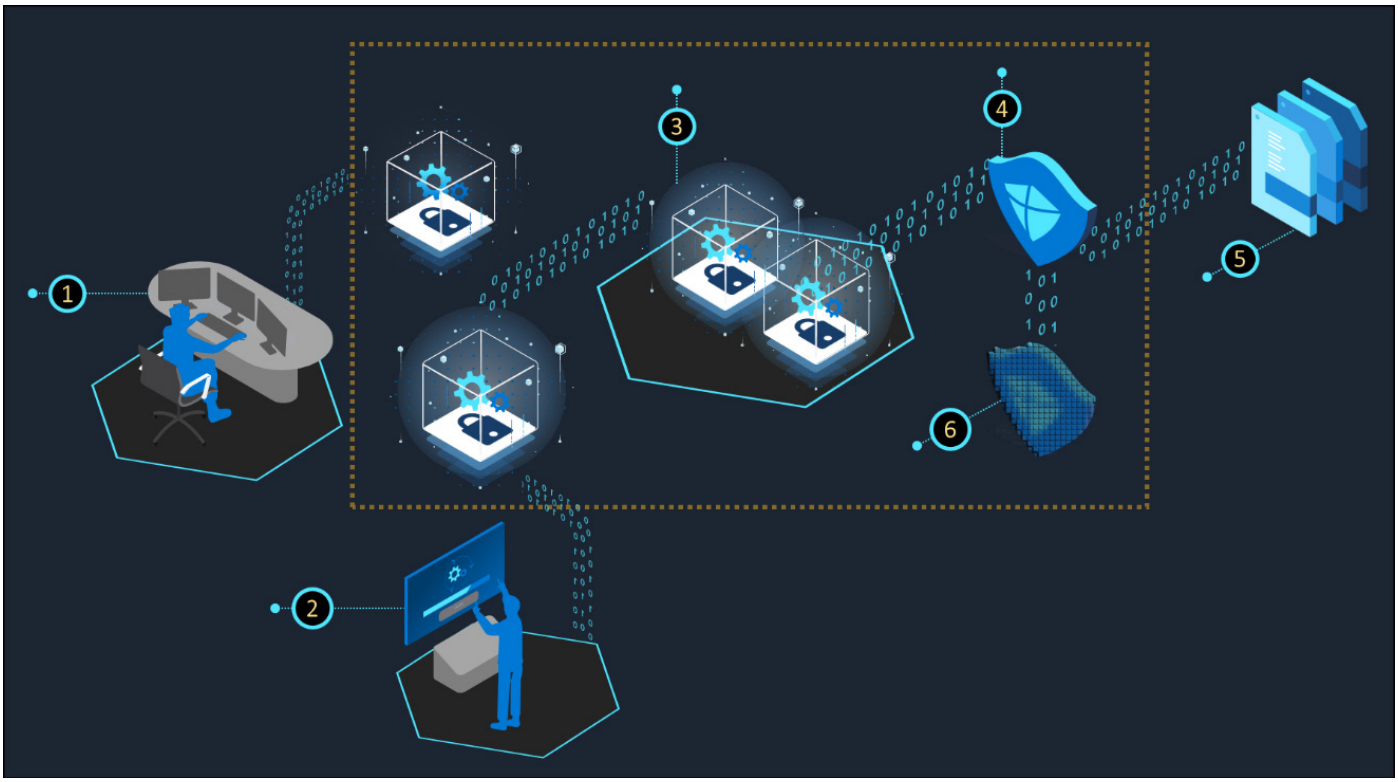
Challenge: Lack of data availability for healthcare AI validation is stifling innovation and improvement in patient outcomes

Healthcare artificial intelligence (AI) is estimated to improve healthcare outcomes by 30-40% while reducing treatment costs by as much as 50%.[1] However, achieving these improvements with AI models requires that algorithm developers gain access to sufficient data with the correct features representing the variation expected in real world settings. In today's environment it can take up to 3 years and $3-5 million[1] to secure access to historical data and then train a model until it achieves a consistent level of performance in data sets of dissimilar distribution (i.e., generalizability).

Solution: Privacy-preserving confidential computing on the BeeKeeperAI platform enables collaboration between data stewards and algorithm owners and accelerates validation of Healthcare AI

The BeeKeeperAI platform allows data stewards to keep their sensitive data in their HIPAA compliant cloud environment while still pursuing their mission to advance healthcare discovery and delivery. The platform allows algorithm developers to bring their models into a federated selection of data stewards' HIPAA-compliant cloud environments to run against encrypted data within a secure computing enclave. Processing within the secure enclave guarantees that AI developers cannot see the data and the data stewards cannot discover the algorithm's intellectual property. BeeKeeperAI ensures that the computational results (e.g., confidential algorithm performance report, model performance, inferences, etc.) adhere to the confidentiality requirements specified by the algorithm developer and data steward.

Once an algorithm is deployed and is running on real-time prospective data, there is a need to monitor the algorithm for performance drift as it encounters new data. If this does not occur, healthcare providers utilizing the algorithms will abandon the AI as it begins to perform poorly.



How It Works

BeeKeeperAI designs security into the foundation of the platform – not as an afterthought – providing protection that eliminates the need for implicit trust while providing continuous validation at every stage of a digital interaction. This facilitates secure, sightless computing on Protected Health Information (PHI), as illustrated above.

1. An algorithm owner submits their encrypted algorithm to the BeeKeeperAI platform. Their algorithm is wrapped in a secure computing container.
2. A data steward curates a data set to meet the algorithm owner's requirements. The data set is encrypted and uploaded to a BeeKeeperAI accessible zone within their secure compliant cloud.
3. To validate the algorithm, BeeKeeperAI brings the secure container into the data owners' compliant environment where it is merged with the encrypted data in an attested Intel® SGX compute enclave.
4. With the enclave attested, the algorithm and data are decrypted in the Intel SGX-protected memory. The algorithm runs, and a confidential report is created containing the algorithm's performance and the general characteristics of the data set.
5. That performance report is the only thing that leaves that secure computing enclave.
6. Then all the elements within the enclave are destroyed, and the enclave is depermissioned.

"As the former Chair of the IT Security committee at UCSF, I developed a deep appreciation for the need to secure our data while making it available to advance the mission of the organization."

Michael Blum, MD
Co-founder and CEO
BeeKeeperAI

Solution Summary

Using BeeKeeperAI's privacy-preserving collaboration platform, data stewards can pursue their mission of improving patient care through research and discovery without sharing patient data or risk exposing PHI. Algorithm developers can securely train and validate their algorithms without worrying about the security of their intellectual property. Patients' privacy is always maintained.

- **Regulatory Compliant.** Secure Enclave Node is enrolled into a HIPAA compliant network using a one-time token issued to an authenticated organization administrator. A third-party audit deemed BeeKeeperAI HIPAA compliant due to the use of a full change log and audit trail for all critical system processes.

- **End-to-end Encryption.** Data and algorithm are encrypted at rest, in transit, and during computation. Nothing is decrypted until containers are merged within an attested and secure Intel SGX enclave.
- **Privacy-Preserving and Sightless Computing.** No one can observe the run time contents of the secure compute enclave.
- **Control-at-all-Times.** Client-side encryption preserves control by data stewards and algorithm owners. Keys can be changed at any time and can only be provided to an attested compute enclave authorized by the enclave publisher.

> *"Now we are able to help AI algorithm developers find the data stewards they need to validate their models."*
>
> **Mary Beth Chalk**
> Co-Founder and Chief Commercial Officer
> BeeKeeperAI

Industry-leading Intel technologies

BeeKeeperAI leverages the industry-leading security capabilities delivered by Intel® Software Guard Extensions (Intel® SGX). Intel SGX consists of a set of security features built into 3rd and 4th generation Intel® Xeon® Scalable processors. Designed specifically to support trusted computation, Intel SGX enables developers to partition code into hardened enclaves. Data processed inside an enclave is invisible to other applications, the operating system or hypervisor, and even rogue employees with credential-enabled access.

Originally designed for general remote computation security, secure web browsing, and digital rights management, Intel SGX has expanded to support AI workloads that have moved to the cloud. BeeKeeperAI works with Intel SGX and its hardware-based memory encryption to isolate specific application code and data. Thanks to Intel SGX, multiple organizations can more confidently work together to validate algorithms while better protecting their intellectual property and data.

The combination of BeeKeeperAI features and the power and functionality of Intel technology opens new possibilities for healthcare groups seeking to benefit from the security of confidential cloud computing.

Potential Deployments

- Medical device diagnostic algorithm validation for regulatory clearance submission
- Clinical decision support software inference validation
- Healthcare AI deep learning training
- Pharmaceutical post market surveillance

About BeeKeeperAI

BeeKeeperAI is the pioneer in combining zero trust, confidential computing, and privacy preserving-analytics for the training, validation, and deployment of artificial intelligence (AI) in healthcare. BeeKeeperAI is accelerating the broader availability of AI-powered solutions that will help to redefine the future of healthcare.

Getting Started with BeeKeeperAI

To get started benefiting from BeeKeeperAI, go to beekeeperAI.com.

Learn More

BeeKeeperAI
https://www.beekeeperai.com/

Intel® SGX
https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html

1 Intel® Vision 2021, Greg Lavender
Alder S. (2022, January 18). December 2021 Healthcare Data Breach Report. HIPAA Journal. https://www.hipaajournal.com/december-2021-healthcare-data-breach-report/.
IBM. (2021). Cost of a Data Breach Report 2021.
Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
ACG6287FSB