anjuna

WHITEPAPER

Alignment of Confidential Computing with Data Protection Standards in the Healthcare Industry

Executive Summary

Confidential Computing is a rapidly expanding technology category that plays a crucial role in ensuring compliance with data protection standards and regulations by providing a secure environment for processing sensitive information. By leveraging Trusted Execution Environments (TEEs), Confidential Computing ensures that data is encrypted and protected even while in use, mitigating the risk of unauthorized access or exposure. This level of security helps organizations adhere to stringent data protection regulations which require robust measures to safeguard sensitive data. With Confidential Computing, organizations can confidently process and analyze sensitive data while maintaining compliance with regulatory requirements, ultimately fostering trust and confidence among customers and stakeholders.

Anjuna Seaglass is a Universal Confidential Computing Platform that further enhances the compliance capabilities of organizations by offering a comprehensive approach to security, automation, and ease of deployment. To enhance the security posture, it orchestrates TEEs in a way that allows data to be protected in every state, not only while in use, but also in transit as it leaves the secure enclave and at rest as it reaches persistent storage. To simplify and accelerate deployment, Anjuna Seaglass virtualizes modern Confidential Computing processors available on all the leading clouds: AWS, Azure and Google Cloud. By abstracting away the complexity of the underlying infrastructure, Anjuna Seaglass enables running any application - traditional, containerized, or Kubernetes-managed – in a matter of minutes (without the need to rearchitect), with a consistent operational model across clouds.

This document outlines how Anjuna Seaglass aligns with and supports compliance with various global data protection and privacy regulations. These regulations include the **Health Insurance Portability and Accountability Act (HIPAA)** and the **Health Information Technology for Economic and Clinical Health (HITECH) Act** in the United States, the **Food and Drug Administration's (FDA)** criteria under 21 CFR Part 11, the **General Data Protection Regulation (GDPR)** in the European Union, and various country-specific **Personal Data Protection Acts (PDPA)** in Asia.

U.S. Based Regulatory Bodies:

HIPAA (Health Insurance Portability and Accountability Act) - 45 CFR Parts 160, 162, and 164: HIPAA sets the standard for protecting sensitive patient data. It requires appropriate safeguards to protect the privacy and security of health information

HIPAA Requirement	Description of Requirement	Anjuna Seaglass Alignment	Impact Level
Administrative Safeguards (§164.308)	Policies and procedures to manage security measures' selection, development, implementation, and maintenance.	Anjuna Seaglass supports the deployment of policy-based controls through the measurement of applications, utilizing these metrics to secure keys and configurations. This approach ensures the foundation for implementing access management and risk assessment capabilities is robust, meeting the necessary administrative safeguards. Through this method, Anjuna enables organizations to manage and protect sensitive information effectively, aligning with the highest data security and compliance standards.	Medium
Physical Safeguards (§164.310)	Measures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.	While Anjuna primarily focuses on software solutions, its encryption and secure enclave technologies indirectly support physical safeguards by ensuring data security regardless of the physical state of the hardware. Theft of servers presents no risk of compromise with a confidential computing secure workload.	High
Technical Safeguards (§164.312)	The technology and the policy and procedures for its use that protect electronically protected health information and control access to it.	Encryption and Decryption (§164.312(a)(2)(iv)): Anjuna Seaglass' encryption in-use, at-rest, and in-transit ensures data is always protected. Access Control (§164.312(a)(1)): Secure enclave technology and attestation ensure that only authorized personnel access PHI. Audit Controls (§164.312(b)): Anjuna enables detailed logging for monitoring and auditing access to PHI.	High
Data De-Identification §164.514(a)-(b)	Data redaction, de-identification, expert opinion, or safe harbor method.	Where consent for data processing has been obtained, confidential computing allows full-fidelity data operations and AI to be processed in a confidential computing environment isolated from IT attacks, CSPs, and attacks. This ensures processing privacy with hardware isolation, enabling full HIPAA privacy compliance without complexity. To process data, including the 18 HIPAA identifiers, organizations utilize data masking, synthetic data, or encrypted data. However, any process performing data de-identification, for example, an AI-based model that learns from a data set and re-synthesizes the data, must also operate with absolute integrity with proof to withstand scrutiny under audit. A software-only approach that can be compromised or subject to insider access or attack may have issues including a) access to the precise data in advance during training, which enables re-identification of synthetic data back to original data, or b) the process of creating synthetic data itself may be compromised, resulting in downstream synthetic data having fewer security properties than desired. By running this in confidential computing, guarantees of integrity based on hardware are achievable, providing far stronger assurances over the generation of HIPAA Identifiers for storage, processing, and operation.	High

HITECH Act (Health Information Technology for Economic and Clinical Health Act) - Public Law 111-5: The HITECH Act expands the scope of privacy and security protections under HIPAA, including the requirement for breach notification in case of unauthorized access to protected health information.

HITECH Act Requirement	Description of Requirement	Anjuna Seaglass Alignment	Impact Level
Expanded Security Provisions for PHI	Enhances HIPAA's security measures to ensure PHI's integrity, confidentiality, and availability.	Anjuna Seaglass' encryption and secure enclave technologies protect PHI at all stages (in-use, at-rest, in-transit), aligning with the enhanced security provisions by ensuring data is safeguarded against unauthorized access.	Medium
Breach Notification Protocol	Requires covered entities and their business associates to provide notification following a breach of unsecured PHI.	Although Anjuna does not directly manage breach notifications, its automated termination features and restrictions on lateral movements play a crucial role in mitigating breach risks. By promptly isolating and terminating unauthorized access attempts, these mechanisms effectively reduce the likelihood of incidents that would necessitate breach notifications. This contributes to compliance efforts by decreasing the frequency of incidents that require reporting.	High
Enhanced Penalties for Non-Compliance	Introduces increased penalties for non-compliance with HIPAA and HITECH Act provisions.	Anjuna Seaglass provides a robust framework that helps healthcare organizations prevent violations by securing PHI effectively, thereby aiding in compliance and avoiding the increased penalties associated with non-compliance.	High
Business Associate Agreements (BAAs)	Extend the HIPAA requirements to business associates, requiring them to comply with HIPAA's Privacy and Security Rules.	Anjuna Seaglass can be extended to business associates, ensuring that they can protect PHI in accordance with HIPAA and HITECH requirements facilitating compliance through technology that secures data across multiple parties.	Medium

The **FDA's 21 CFR Part 11** guidelines ensure electronic records and signatures are as reliable as paper ones, which is important for managing clinical trial data and patient information. The recent FDA update highlights confidential computing's role in data security, leveraging Anjuna's hardware-based isolation to secure data and AI models, streamline compliance, and modernize clinical trials with AI.

21 CFR Part 11 Requirement	Description of Requirement	Anjuna Seaglass Alignment	Impact Level
Integrity and Confidentiality of Electronic Records	Electronic records must be maintained to ensure their integrity, authenticity, and confidentiality.	Anjuna Seaglass' encryption and secure enclave technology safeguard the integrity and confidentiality of electronic records, ensuring they are as trustworthy and reliable as paper records. This technology provides a secure environment that protects clinical trial data, patient health records, and other medical information from unauthorized access or alterations.	Medium
Electronic Signatures	Electronic signatures must be as reliable, trustworthy, and generally equivalent to handwritten signatures.	By employing secure enclave technology, Anjuna Seaglass ensures that electronic signatures are protected and managed securely, maintaining their authenticity and non-repudiation. This meets the FDA's criteria for electronic signatures, making them equivalent to handwritten signatures in their reliability and trustworthiness.	High
Access Controls and Key Management	Systems need robust access controls and secure encryption key management to ensure only authorized access to electronic records and signatures.	Anjuna Seaglass leverages secure enclave technology to protect key management and strict access controls, ensuring that encryption keys are well-protected and that only authorized users can access electronic records or execute electronic signatures. This directly supports the FDA's requirement for secure access and key management, thereby ensuring the security and integrity of electronic records and signatures.	High
Software Integrity and Configuration Attestation	The software used to generate, manage, and store electronic records and signatures must be verified for integrity and secure configuration.	Anjuna Seaglass leverages attestation to verify software's integrity and secure configuration, managing electronic records and signatures. This ensures that only authorized and validated software can access and process medical information, aligning with the FDA's standards for the trustworthiness and reliability of electronic records.	High

E.U. Based Regulatory Bodies:

GDPR (General Data Protection Regulation) - Regulation (EU) 2016/679: GDPR sets strict requirements for protecting personal data, including health information. It requires organizations to implement appropriate technical and organizational measures to ensure the security and confidentiality of personal data.

GDPR Requirement	Description of Requirement	Anjuna Seaglass Alignment	Impact Level
Data Protection by Design and by Default (Article 25)	Requires that data protection measures are integrated into the development of business processes for products and services.	Anjuna Seaglass' encryption and secure enclave technologies ensure data protection from the ground up, encrypting data at all stages (in-use, at-rest, in-transit) and meeting the GDPR's data protection principle by design and by default.	High
Processing Integrity and Confidentiality (Article 5(1)f)	Personal data must be processed to ensure its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.	Anjuna Seaglass utilizes secure enclave technology and attestation to verify the integrity and security of the software environment processing personal data. This aligns with GDPR's requirements for maintaining processing integrity and confidentiality, ensuring that only authorized and trustworthy applications handle personal data.	High
Technical Safeguards (§164.312)	Requires the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including encryption and access control.	Anjuna Seaglass' comprehensive data encryption and secure enclave technology for data protection and access control directly support GDPR's mandate for technical and organizational measures, providing robust security mechanisms to protect personal data against unauthorized access and ensuring the confidentiality and integrity of data processing.	High
Data Access Control	Ensures that access to personal data is restricted to authorized personnel, with mechanisms in place to prevent unauthorized access.	Anjuna Seaglass enforces stringent access controls and key management in secure enclaves, allowing only authorized users to access and process personal data, aligning with GDPR's mandate to restrict data access to legitimately authorized individuals.	High

Additional Global Regulatory Bodies:

PDPA (Personal Data Protection Act) - Various country-specific laws: Asian countries have enacted their own versions of data protection laws, such as Singapore's PDPA. These laws regulate personal data collection, use, and disclosure, including health information.

PDPA Requirement	Description of Requirement	Anjuna Seaglass Alignment	Impact Level
Comprehensive Data Protection	PDPA laws mandate the protection of personal data from unauthorized access, use, or disclosure throughout its lifecycle.	Anjuna Seaglass encrypts data in all stages: in-use, at-rest, and in-transit, providing robust protection against unauthorized access and data breaches. This comprehensive approach ensures healthcare organizations can maintain the confidentiality and integrity of patient data, directly aligning with PDPA's data protection mandates.	High
Protection of Sensitive Health Information	Many PDPA regulations emphasize the need for special care in handling sensitive health data, requiring enhanced security measures.	Anjuna Seaglass offers in-memory protection for sensitive health data, ensuring that it is encrypted and isolated from other processes. This level of protection is critical for meeting the PDPA's emphasis on the security of health information during processing, effectively preventing unauthorized access or data leaks.	High
Access Control and Integrity of Data Processing	PDPA emphasizes strict access controls and transparent, lawful data processing activities to ensure the security and integrity of personal data.	Through the use of attestation, Anjuna Seaglass verifies the integrity and security of software environments accessing and processing personal data. This ensures that only authorized applications and processes can manage sensitive data, supporting PDPA's requirements for lawful data use and transparent processing activities by enforcing strict access controls and verifying data processing integrity.	High

About Anjuna Seaglass

Anjuna Seaglass™ is the world’s first Universal Confidential Computing Platform, capable of running applications in any cloud with complete data security and privacy. Anjuna Seaglass isolates workloads in a hardware-assisted Trusted Execution Environment that intrinsically secures data in every state – in use, at rest, and in transit – to create a zero trust environment.

Get Started

REV-0524