EZEC's Commitment

EZEC works with many organizations who may be defined as a Covered Entity under HIPAA or may be required to act as a Business Associate under HIPAA. EZEC has undergone a comprehensive review of all administrative, technical, and physical safeguards to ensure the protection of e-PHI.

This includes:

1. Ensuring the confidentiality, integrity, and availability of all e-PHI created, received, maintained, or transmitted.
2. Identifying and protecting against reasonably anticipated threats to the security or integrity of information.
3. Protecting against reasonably anticipated impermissible uses or disclosures.
4. Ensuring compliance within our workforce.

EZEC is also Genera Data Protection Regulation GDPR compliant. This is a set standard of regulations and law on data protection and privacy in the European Union, important to privacy and human rights. This also addresses the transfer of personal data outside the EU and EEA areas. The California Consumer Privacy Act of 2018 has many similarities with GDPR.

EZEC has a set standard of compliance with all our technical, operational, and administrative systems. We set standards to be 'compliant by design' and uphold 'privacy by default'. HIPAA compliance and GDPR standards provide an additional layer of security in handling any personal healthcare data that may pass through our systems.

Security Controls

EZEC has implemented necessary measures to ensure HIPAA compliance for administrative, physical, and technical controls. We enable the safe, ethical, compliant, and efficient development of life-changing access to medical information.

Risk Assessment – As part of our Compliance and Security Management process; we conduct annual risk assessments which include the likelihood and impact of potential risks. This helps ensure that controls are appropriate to meet the needs of our organization. By conducting these annually, we ensure our organization continues to provide the highest level of data security that has been developed, entrusted, and protected.

Administrative Safeguards – We operate in compliance with various guidelines as applicable including, but not limited to, the Federal Information Security Management Act, ISO 22301, ISO/IEC 27001, ISO/IEC 27032, ISO 27701, and guidelines set forth which address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. We also follow various global guidelines as applicable (both domestic and international) including, but not limited to HIPAA, GDPR, federal geolocation privacy laws, and the ethical principles of human rights.

We have developed a security management process including appropriate standard operating procedures (SOP's) and policies. A Security Manager, Compliance Officer, and Information Data Specialist are assigned to help develop and review policies and procedures. Staff are kept up to date and trained on HIPAA security annually. Internal review of these safeguards is performed regularly to ensure compliance and reviewed for continual improvement.

Physical Safeguards – EZEC ensures the data storage of electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers, hard drives, and any removable and/or transportable digital memory medium such as disks or memory cards; have implemented strict state of the art security systems. We maintain strict policies to ensure e-PHI is only housed in secure locations with restricted access. Our facilities are wired with a high level of security and are UL certified compliant. Transmission media is also under strict monitor and control.

Transmission media is used to exchange information already in electronic storage such as, for example, the internet, extranet or intranet, leased lines, dial-up likes, private networks, and the physical movement of removable and/or transportable electronic media. Other transmissions, including paper via facsimile, voice, via telephone, are not considered to be transmission via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission. EZEC strictly follows the definitions and general provisions required in 45 CFR § 160.103 Subpart A.

Technology Safeguards – We have implemented appropriate technology safeguards to authenticate and authorize our employees for appropriate use of our software and applications access. We maintain appropriate auditing and integrity controls. Appropriate data controls, data encryption, and other systems are implemented when appropriate to ensure the highest level of security for our organization.

HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) defines a set of regulations that protect the privacy and security of certain health information. The Department of Health and Human Services (HSS) has published what is commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

The Privacy Rule, commonly known as the Standards for Privacy of Individual Identifiable Health Information (PHI), establishes national standards for the protection of certain health information. The goal for the Privacy Rule is to provide an individual adequate notice how a covered entity might use and disclose protected health information about them.

The Security Rule establishes standards for the protection of electronic protected health information that is held or transferred in electronic format. A major goal of the Security Rule is to protect the privacy of individuals/ health information while allowing covered entities to use new technologies to improve the quality and efficiency of patient care. With such a diverse health care network of technology language and software, the Security Rule is designed to be flexible and scalable so a covered entity can implement policies, procedures, and technology that is appropriate for the entity's particular size, organization structure, and risks to an individual's e-PHI.

Compliance

Further information on our specific policies and procedures are available upon request. The information regarding HIPAA compliance is for informational purposes only and is not meant as a form to convey, warrant, or represent a guarantee of any kind. We encourage the use of Business Associate Agreements to address specific compliance requirements. For further information, please contact our Compliance Department at compliance@myezec.com

(The remainder of this page intentionally left blank)