Statement of Privacy Practices

ZCI Claims Integrity, Inc. (referred to as ZCI) is committed to protecting the privacy and confidentiality of all forms of patient information (collectively referred to as Protected Health Information or PHI) received and maintained by us. ZCI's policies and procedures are designed to meet or exceed the physical and electronic security measures required by applicable federal and state regulatory guidelines for the use, storage and/or transmission of PHI. ZCI has implemented electronic and physical security policies and procedures to protect patient information from unauthorized access, improper use, alteration or accidental destruction. In all aspects of its business, ZCI strives to strictly adhere to our Privacy and Security Policies and Procedures and all applicable laws, including the privacy and security regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 and as modified by the HITECH Act of 2009.

Data Security

ZCI has adopted the following safeguards to help ensure that PHI is protected:

- SSL Technology and Encryption. ZCI uses Secure Socket Layer (SSL) technology in areas of our website applications that require data/information transmission. Evidence of SSL activation includes a padlock symbol display at the bottom of the Internet Explorer window or bottom left corner of Netscape Navigator and the URL (web site address) changing from "http" to "https." SSL encryption verifies identity and prevents altering and interception of data being accessed. ZCI uses a Global Server ID that provides a minimum of 128-bit SSL encryption and can support 256-bit SSL encryption. Additionally, all portable physical devices and/or media, including back-up media, containing PHI are encrypted in order to protect data in motion and at rest. Laptops and desktops that are used for the processing of sensitive information have been configured to disable the computer from storing information on the USB Flash drives to eliminate the potential for the theft of large amounts of confidential or sensitive data.
- State of Art Data Center. ZCI servers, containing all stored PHI are located within our secure data center. Our facility utilizes access cards to ensure that only authorized personnel have access to ZCI's systems. All visitors accessing the data center must sign the Data Center Visitor Log and be accompanied by an authorized ZCI employee.
- Password and ID Protections. Through proprietary software applications, ZCI controls access to restricted areas of our applications and databases via login authentication, which requires a username, account ID and password be provided before access is granted. Unique user names, account IDs and passwords are assigned and distributed only to authorized ZCI personnel and or customers' personnel as directed by our customers. This login process not only regulates who gains access, but also limits the scope of access. Once a user is logged in, their access is limited to only the data for which they are authorized. An automatic log off feature prevents unauthorized access to information if the original user leaves the workstation without logging off.
- Self-Assessments and Security Audits. ZCI records and regularly reviews all system activities, including but not limited to, logins, file access and security events. ZCI uses this audit system to assess and critique our technical security measures. ZCI has also implemented technical and administrative procedures to ensure that hardware and software enhancements do not compromise data security.

Data Privacy

- Limitation of uses. ZCI utilizes and discloses protected health information received from its customers only for the limited purposes set forth in its agreements with each customer.
- Customer responsibilities.
    - Data submission and revision obligations. ZCI relies solely on the customer to provide accurate and up-to-date patient data. Once received by ZCI, we will ensure the integrity and security of the data is maintained in accordance with the policies summarized herein. ZCI employs various processes to ensure that data remains as it was as originally received from the customer.
    - Customers control what information is provided to ZCI and can choose to omit any information not necessary or applicable. Customers must determine what is or is not appropriate to provide to ZCI, and whether additional patient consent is required, in accordance with the purposes for which the customer is utilizing the information.
    - It is the customer's responsibility to request (in writing) removal of any PHI from ZCI's data center if necessary to comply with patient requests. ZCI will respond expeditiously to any such request, but advance notice is required as such data modifications may require significant time and resources, depending upon the complexity of the request.
- Retention and Disposal of Protected Health Information. The protected health information submitted by customers to ZCI is not a medical record nor a designated record set as defined by HIPAA and, therefore, ZCI shall have no obligations to maintain this information as a medical record in accordance with state or federal laws.
    - ZCI shall retain all protected health information submitted by customers in accordance with written customer agreements and ZCI data retention policies. To the extent data is destroyed, it is destroyed in accordance with applicable industry standards to protect identifiable data from theft, misuse or unauthorized access.
- Patient Access. ZCI is solely a business associate of our customer. ZCI does not grant patients direct access to their protected health information. Should a patient have questions or need access for some reason, ZCI will work with the customer to provide appropriate responses and access. To the extent ZCI receives a request from a patient, a patient's legal representative, or other legal authority to access data within any ZCI database, ZCI will notify the customer and work cooperatively to provide information in a legally appropriate manner.
- Collection of Customer Information. ZCI does not collect or utilize any other data about its customers or customers' patients.

Customer Agreements

- ZCI enters into a HIPAA/HITECH Act-compliant Business Associate Agreement or Business Associate Subcontractor Agreement with each of its customers, which provides further acknowledgements of ZCI legal and contractual obligations and commitments to comply with state and federal laws.

Third Party Vendors

- ZCI utilizes, on a very limited basis, the services of third party vendors that require such third parties to access protected health information. Where such relationships exist, ZCI enters into subcontractor Business Associate Agreements requiring the vendor to comply with all business associate obligations imposed by state and federal law.

Personnel Training and Compliance Enforcement

- ZCI requires initial training of all new staff as well as an annual on-going refresher training on ZCI Privacy and Security Policies and Procedures for existing staff with exposure to PHI. Employees are trained to recognize security concerns and report those immediately to ZCI management. ZCI limits PHI access to only those employees who need this information in order to perform their duties in accordance with our contractual obligation to our customers. Compliance is diligently monitored and violations are dealt with immediately.

Questions/Reporting of Concerns

- Specific questions, inquiries, complaints and disputes about ZCI's Privacy or Security Policies and Procedures can be directed to your client services representative or ZCI privacy officer:

  Suman Sethi

  2 Crossroads Drive

  Bedminster, NJ 07921

  1-908-444-0396

  suman.sethi@zelis.com

This version of the ZCI Statement of Privacy Practices is as of October 2016 and supersedes any earlier versions.

Thank you for being part of the ZCI Community.

Approved Date: October 2016