AMALGAMATED FAMILY OF COMPANIES, ALICARE, INC, AND ALICARE MEDICAL MANAGEMENT
(collectively referred to herein as the "Amalgamated Family of Companies")

POLICY & PROCEDURE

SUBJECT: HEALTH INSURANCE PORTABILITY AMENDMENTS ACT (HIPAA) COMPLIANCE

DATE: MAY 2015

POLICY: It is the policy of Amalgamated Family of Companies (herein the "Company") to ensure that all employees within the organization who come in contact or work with protected health information comply with the rules and standards established by the government, or where more restrictive, the standards developed at the Company, regarding the proper handling, maintenance and transmission of this type of information.

SCOPE: The following rules and procedures of the Company are pursuant to the Security Regulations of the Health Insurance Portability Amendments Act (HIPAA) Security Regulations (herein the Regulations) Any ambiguity in these Procedures shall be resolved in such a fashion so that these Procedures meet the minimum requirements of the Regulations.

Unless otherwise expressly indicated the terms used herein, if defined in the Regulations, shall have the definition given to them by the Regulations.

Security Standards

These Procedures are adopted to:

1) Ensure the confidentiality, integrity, and availability of all protected health information and Personally Identifiable Information (collectively referred to as PHI) created, received, maintained, or transmitted by the Company;
2) Protect against any reasonably anticipated threats or hazards to the security or integrity of the PHI;
3) Protect against any reasonably anticipated uses or disclosures of the information that are not permitted or required by the HIPAA Privacy Rules;
4) Ensure workforce compliance.

An employee that fails to comply with these Procedures shall be deemed to have violated a Company policy and shall be subject to disciplinary action to the same extent as a violation of any other Company policy or work rule.

Administrative Safeguards

On an annual basis the Company performs assessments of all systems and networks for security risks and vulnerabilities to the confidentiality of PHI. Changes will be made, if and when necessary to prevent, detect, contain, and correct future security violations or to reduce them to an acceptable level.

The Company's Security Manager shall be responsible for developing and implementing the procedures required by this policy.

On an annual basis the Company shall review the access rights of all employees with access to PHI; and on a periodic basis, the Company will ensure that each employee is given access only to the PHI necessary to perform his/her job role.

Workforce Security

The following Procedures are designed to ensure that all workforce members have only appropriate access to PHI, and to prevent those who do not have access from improperly obtaining access to PHI.

1) All employees with access to PHI shall be required to employ a unique employee password to obtain access to PHI. The password assignment shall be in accordance with the polices and procedures established by the Company to comply with the Privacy Regulations of the Health Insurance Plan amendments Act (the Privacy Rules) which are incorporated herein by reference with the same force and effect as if set forth at length herein.

2) Workforce clearance procedure – No employee shall be given a password unless and until there has been compliance with Company's Privacy Rules relating to the assignment of passwords.

3) Termination procedures – When an employee ceases to be an employee of the Company for any reason his or her access to PHI shall be terminated and his password shall be deactivated so that the use of it will no longer allow access to PHI.

Information Access Management

1) Access authorization – No employee will be granted access to any PHI unless and until an access form, as required under the Company's Privacy Rules, has been completed and submitted.

2) Access establishment and modification – On annual periodic basis every manager shall notify Information Technology if an employee's access to PHI requires a modification.

Security Awareness and Training

1) Security reminders – On an annual basis every employee with access to PHI shall be given a reminder of the need to comply with security and privacy rules and,

when applicable, with a notice of any change in the Company's rules, policies or procedures.

2) Protection from malicious software – To guard against, detect and report malicious software the Company shall continue the use of Enterprise Level Anti-Malware software, the use of a firewall and the policy of scanning all e-mails prior to their delivery.

3) Log-in monitoring – The Company will continue its policy of automatically locking out any attempted user that has five unsuccessful attempts at logging in and will not allow that access point or user to have access to PHI unless and until the user can provide evidence of his or her right and authority to access PHI.

4) Password management – The Company will continue its policy of requiring users to change their password every ninety- (90) days. Employees will be reminded periodically not to share their password with any other person, including other employees.

Procedures In The Event of An Impermissible Disclosure of PHI

In the event that any employee becomes aware of a suspected or possible impermissible disclosure of PHI, the employee will be required to report the disclosure to his or her immediate supervisor. By way of example, an impermissible disclosure may include, but is not limited to, unsecured emails containing PHI sent to recipients outside the Company and correspondence containing PHI inadvertently mailed (via email or regular mail) to an unauthorized third party. Upon learning of the disclosure, the supervisor shall notify the Privacy Officer who, in consultation with Compliance Counsel, shall promptly investigate the circumstances surrounding the disclosure and involve any other Company representatives as necessary. Depending on the results of the investigation, the Privacy Officer, or his/her designee, will contact relevant Company counterparts to inform them of the incident and assist with Company's reporting/notice obligations in the event the disclosure amounts to a HIPAA Breach. The Privacy Officer will maintain documentation of all impermissible disclosures and/or HIPAA Breaches and the corrective action taken to address such incidents.

Contingency Plan

The policies and procedures for responding to an emergency that damages systems containing PHI are as follows:

1) Data backup plan – All PHI shall be backed up daily and the backup copy shall be stored at a location different than the Company's office.

2) Disaster recovery plan – The Disaster Recovery Plan, which includes the procedures for recovering lost or damaged PHI shall be maintained by the Company on its RPX site.

3) Emergency mode operation plan – The procedures to enable continuation of critical business processes and for protection of PHI while operating in emergency mode shall be set forth in the Disaster Recovery Plan.

4) Testing and revision procedures – The Contingency and Disaster Recovery plans shall be reviewed no less frequently than annually and shall be tested at the discretion of the CIO. In the event that the CIO determines, as a result of the review or test that the Contingency Plan or Disaster Recovery Plan needs to be amended the CIO shall assign the requirement to document the need before the revision and shall implement the revision as soon as administratively practical but in no event more than one year after the need to make the change is documented.

Business Associate Agreements and other Arrangements

All entities with whom the Company shares or provides PHI shall be required to enter into a Business Associate Agreement (BAA). The BAA sets forth assurances between business associates, covered entities, and where applicable subcontractor vendors, that all parties will appropriately safeguard the PHI they transmit, receive or create. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity, business associate, and where applicable subcontractor vendors.

Physical Safeguards

Facility Access Controls: Physical access to electronic information systems shall be limited as follows:

1) Contingency operations – The procedures set forth in the Disaster Recovery Plan will be followed to recover data in the event the Company needs to operate in an emergency mode.

2) Facility security plan – The Company's servers shall be kept in a cage secured by a double lock requiring the use of a password and physical key to unlock to safeguard the facility and its contents from unauthorized access, tampering and theft.

3) Access control and validation – The use of passwords shall be required in order to validate access to facilities based on a person's role.

4) Maintenance records – Records shall be kept to track access to the physical facility for the purpose of maintaining or repairing the facility with respect to security matters.

Workstation Use: Use of and access to PHI by use of a workstation shall be limited in accordance with the Company's Privacy Rules.

Workstation Security: Workstation access shall be limited by use of required passwords. Employees shall be educated in the use of passwords including the requirement to update them every ninety-(90) days and the need to keep them confidential.

Device and Media Controls: The policies and procedures set forth in The Company's Privacy Procedures apply to the receipt and removal of hardware and software that contain PHI, and their movement within the Company's physical facility.

Portable, Mobile and Removable Storage Devices: The policies and procedures set forth in The Company's Privacy Procedures apply to the use of all company issued portable, mobile and removable devices that have storage capacity, such as but not limited to: USB Storage drives, Laptops, Smart Phones and External Hard Drives. Storage and transport of PHI will NOT be allowed on any non-company provided device without prior written authorization and the assurance that the device is secured with a minimum of HIPAA FIPS 140-2 level encryption.

Technical Safeguards

Access Control: The Company shall limit access to PHI to only those people who require such access to perform their job function.

1) Automatic logoff – All workstations that can access PHI shall be programmed to automatically logoff any systems containing PHI if there has been no activity from the workstation after a three minute period.

2) Encryption and decryption – All eligibility data received or sent by the Company by EDI shall be encrypted. E-mails will be sent on a secure server. Employees are unable to place any indication in the subject line of an e-mail that the e-mail may contain PHI through system controls.

Audit Controls: The Company will continue to monitor employee access rights to PHI to ensure that employees continue to have access only to PHI that is appropriate for the employee's job function.

Integrity: To insure that PHI is not improperly altered or destroyed the Company will follow the procedures set forth in the Company Privacy Procedures. When a tiff file is created the original PHI in EDI format shall be stored for comparison purposes.

Person or Entity Authentication: To ensure the reliability of PHI transmissions, PHI shall be sent only by and to secure servers.

Transmission Security: To guard against unauthorized access to PHI that is being transmitted the Company has adopted the following procedures.

1) Integrity controls – To ensure PHI is not improperly modified until disposed of, when tiff files are created copies of the data shall also retained in the original EDI format.
2) Encryption – shall be employed automatically on all files.

Requirements for Group Health Plans

No PHI shall be transmitted to a health plan unless the plan certifies that its plan documents have been amended to authorize it to obtain PHI.