RCB HIPAA Compliance Plan

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule identifies standards and implementation specifications that organizations must meet in order to remain compliant with federal law. The purpose of the security Rule is to adopt national standards for safeguards to protect the confidentiality, integrity and availability of electronic protected health information. All HIPAA *covered* entities must comply with the Security Rule. When one is acting as a business associate (e.g., collection agency) of a covered entity, business associate must protect the electronic protected health information (EPHI) it creates, receives, maintains or transmits on the covered entity's behalf.

RCB's Security policy is divided into **three main categories**: administrative, technical, and physical.

***Administrative** Safeguards & Security Management Process:*

Risk Analysis - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI held by the covered entity.

Risk Management - Implement measures to reduce the security risks to a reasonable and appropriate level.

Sanction Policy - Apply appropriate sanctions against employees who fail to comply with the security policies and procedures established by the covered entity.

Workforce Security:

*For each employee or job function, identify the EPHI that is needed, when it is needed and make reasonable efforts to control the access to the EPHI**.***

Workforce Clearance Procedure - Implement procedures to determine that the access of an employee to EPHI is appropriate. RCB requires all employees to be licensed collectors, credit and criminal bank grounds checked.

Termination Procedures -   Implement procedures for terminating access to EPHI when the employment of a workforce member ends. This does include the deletion of the employee's user account, changing locks/combinations and collection of any company property the employee may have.

*Security (**Technical)** Awareness and Training**:***

The standard requires a covered entity to implement a security awareness and training program for all workforce members, including management.

Security Reminders - Includes notices in printed or electronic forms, agenda items at monthly meetings or reminders posted in affected areas.

Protection from Malicious Software - Implement policies for guarding against, detecting and reporting malicious software.

Log-In Monitoring - Implement procedures for log-in attempts and reporting discrepancies, including how users log onto systems and how they are to manage their passwords.

Password Management - Implement procedures for creating, changing and safeguarding passwords.

Security Incident:

Response and Reporting - Implement procedures to identify and respond to suspected or known security incidents. This includes preserving evidence; mitigating, to the extent possible, the situation that caused the incident and documenting the security incidents and their outcome.

Contingency Plan:

Disaster Recovery Plan - Establish procedures to restore any loss of data. Establish procedures to ensure the continuance of critical business processes that must occur to protect the security of electronic protected health information during and immediately after a crisis situation.

Business Associate Contracts:

Similar to the Privacy Rule requirement, covered entities must enter into a contract or other arrangement with business associates prior to allowing a business associate to create, receive, maintain or transmit EPHI on the covered entity's behalf.

Physical *Safeguards:*

Facility Access Controls - Implement policies and procedures to limit physical access to electronic information systems and our facility where they are housed.

Device and Media Controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI, in and out of our facility.

Data Backup/Storage - Implement daily back up procedures, weekly and monthly data stored in secure off site location.

Transmission Security - Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.