RMS DATA SECURITY OVERVIEW

Research & Marketing Strategies, Inc. (RMS) is committed to protecting the integrity and security of its client data. The organization is continually evolving its IT compliance activities to safeguard client data and minimize the potential for cybercrime. Below are some of the primary means by which RMS seeks to minimize IT breach risks and protect client information assets:

1. Use of FTP and File Sharing Software: The RMS team uses FTP (File Transfer Protocol) data portals that allow for encrypted data in motion to be securely exchanged between the client and RMS.

2. Staff Restricted Server Security Access: Each RMS staff person's position has been evaluated and an appropriate security level has been assigned based upon their job duties. Every employee is provided with unique login credentials and password to access the RMS server system. Client data is not stored on individual computers.

3. Use of Business Associate Agreements: RMS secures Business Associate Agreements with all Healthcare clients and vendors who send and or receive RMS data. The RMS HIPAA Compliance Officer reviews and manages all protocols and policies.

4. RMS Resting Data Encryption: RMS's patient survey PHI data is encrypted when stored on the server. The RMS policy associated with PHI requires that the client data be encrypted, and password protected.

5. Backup and Redundancy Security: RMS maintains data backup through a contracted IT vendor, Kishmish, Inc. (www.kishmish.com) located in Liverpool, NY. RMS has been affiliated with this IT organization since 2004. The firm provides IT consulting for RMS and maintains the server system and backup redundancies which are regularly monitored and tested. Kishmish encrypts the RMS data using a software program, known as Intronis - Barracuda. All data is maintained using AES 256 Encryption. No client data is located, stored or transmitted offshore.

6. Proactive Monitoring: Kishmish proactively monitors the health of all PC based servers and desktops including centrally managing anti-virus software on all desktops.

7. Conduct Vulnerability Audits: RMS contracts with an outside firm to conduct external vulnerability audits to ensure that its firewalls and security activities are robust and reasonable given today's volatile IT cybercrime environment. The most recent audit was conducted by SecurityMetrics®, with future scheduled audits conducted quarterly. Verification of external review has been posted on the RMS website. Additionally, RMS undergoes regular client health system audits to maintain its vendor/subcontractor status with key stakeholders. RMS is held and maintains rigorous security standards required by CMS (Centers for Medicare and Medicaid Services). Validation of compliance is assessed during annual site visits (onsite at RMS).

8. Ongoing Employee Education: As technology continues to advance and data regulations evolve, RMS helps its employees understand their role in data security and IT compliance. This topic along with HIPPA compliance are discussed at monthly staff meetings.

9. Security Policies: RMS retains security policies which reinforce our rigorous commitment to data security. These policies are reviewed and updated annually and are referenced for ongoing employee education. The RMS security policies includes procedures to be undertaken should there be a suspected security breach/incident.

10. Disaster Recovery Plan: RMS maintains a Disaster Recovery Plan. This document details operational procedures should the organization be faced with a sudden, calamitous event that seriously disrupts its functioning. The RMS Disaster Recovery Plan is reviewed and updated annually.

11. Designated HIPAA Compliance Officer: The RMS HIPAA Compliance Officer is Ms. Susan Maxsween. In this capacity, Susan oversees the company's privacy and security compliance to the federal HIPAA policies.

Updated: March 13, 2024