HIPAA SUMMARY

1. Appoint HIPAA Privacy/Security Officer
    a. These positions can be performed by the same person and/or an existing employee, and their first role is to identify where, why, and to what extent PHI is created, received, maintained or transmitted by the group health plan. This will likely involve many different departments such as IT, legal, payroll and HR.
2. Establish a complaint office/practice
3. Implement Privacy Policy
    a. Once the discovery of PHI is completed, the next stage of HIPAA compliance for self-insured group health plans is to develop HIPAA-compliant privacy policies establishing the permitted uses and disclosures of PHI. This should take into account third-party administrators who – as a Business Associate – will also have to comply with HIPAA, and with whom it will be necessary to enter into a HIPAA Business Associate Agreement.
4. If plan receives any PHI electronically, implement a Security Policy, conduct a <u>written</u> risk analysis and establish any necessary safeguards to protect PHI. The written risk analysis should address:
    a. What if any e-PHI is received by plan sponsor
    b. Identification of any vulnerabilities of e-PHI that could lead to disclosure or breach of e-PHI.
    c. Assess administrative, physical and technical safeguards to ensure the integrity of e-PHI
    d. Implement suitable measures and policies to address the vulnerabilities.
5. Establish Breach Notification Policy
    a. Reporting Chain
    b. Notification requirements
6. Make sure plan document has necessary HIPAA provisions
    a. Plan addresses the permitted and required uses of PHI
    b. Sponsor certification that plan documents have been amended to establish the permitted and required uses and disclosures of the PHI by the plan sponsor, a firewall is created to protect the information that is disclosed to the plan sponsor, and that plan sponsor certifies it agrees to the required limitations on the use of the PHI and to meet certain other requirements
7. Conduct employee training.
8. Ensure TPA addressing Notice of Privacy Practices