Personal • Group • Medicare

HAP's Response to Groups Requesting
Data Privacy and Security Assurances

Health Alliance Plan (HAP) is a Covered Entity under the HIPAA Privacy and Security regulations. As such, HAP is obligated under federal law, at the risk of criminal and civil penalties, to comply with all elements of the HIPAA Privacy and Security rules. In addition, its status as a licensed Medicare contractor and as a state-approved health plan in the State of Michigan obligate HAP to a variety of regulatory standards for the custody and protection of customers' data.

HAP's robust compliance program includes the regular review of all privacy and security policies and procedures, and ongoing risk assessments that address each of the HIPAA specifications. Additionally, HAP has a number of security controls in place to protect its ePHI data. These controls include mechanisms to prevent unauthorized access or modification to data within HAP's internal systems and the encryption of all data transmitted outside of HAP's networks.

HAP completed a SOC 1 Type II audit in December 2019 and received a favorable, unqualified opinion. The auditor's report concluded that the controls in place for the core business processing systems are suitably designed to provide reasonable assurance that the specified control objectives would be achieved. Further, the auditors tested HAP's controls and found them to be operating effectively, providing reasonable assurance that the SOC control objectives were achieved.

Various government and industry entities monitor HAP for compliance with a variety of privacy and security standards, including HIPAA. The National Committee for Quality Assurance regularly audits HAP's operations and has never found a deficiency in the programs for protecting customer data. The Office of Civil Rights uses a complaint-driven process to enforce compliance with HIPAA; to date there have been no enforcement actions against HAP.

HAP receives requests for detailed information about its privacy and security programs from numerous purchasers and consultants throughout the year. It is not practical to attempt to comply with the multiple competing requirements suggested by all of these entities. HAP believes it is inadvisable and irresponsible to reveal the type of in-depth information pertaining to system configurations and other controls; such disclosures would ultimately weaken HAP's security position. Therefore, HAP respectfully declines all such requests.