Security Statement

Health Management Associates (HMA) Company Info

HMA is a consulting firm specializing in the fields of health system restructuring, health care program development, health economics and finance, program evaluation, data analysis, and health information technology (HIT) and exchange. HMA is an independent, national research and consulting firm with 23 offices nationwide. HMA has more than 270 consultants.

Information Systems Security Plan (ISSP)

HMA's ISSP establishes an overarching security policy with a set of accompanying policies and designates responsibilities and authorities for ensuring an adequate level of information security for all information collected, created, processed, transmitted, stored, or disseminated on the company's information systems. As part of the ISSP, there must be explicit and well-defined security policies that establish requirements for minimum safeguards, assign roles and responsibilities, provide accountability, and address penalties for noncompliance.

Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)

The BCP process at HMA covers mitigation efforts related to potential short-term and long-term outages or service disruptions. This manual provides guidance on how HMA approaches business continuity planning and establishes the basis for HMA to recover and resume business processes when operations have been disrupted unexpectedly. Processes are in place to ensure disruptions in service are minimized to maintain trust and confidence in HMA systems and business processes. HMA also incorporates business continuity considerations into the overall design of its business model to mitigate the risk of service disruptions.

Data Center Security

HMA utilizes secure Statement on Standards for Attestation Engagements Number 16(SSAE-16) compliant Tier-4 datacenters for network storage of all our electronic data, including a warm site failover for DRP and BCP purposes. All data at rest in the data centers are encrypted and in transit encryption is enabled wherever technically feasible. HMA computers and servers are centrally managed to provide the latest operating system and application security updates, as well as anti-virus (AV) and data loss prevention (DLP) signatures and definitions. The security management systems are checked regularly to ensure all devices have approved software and security releases installed.

Network Security

HMA utilizes next generation firewalls at our data centers and individual sites to provide intrusion detection system (IDS) and intrusion prevention system (IPS) functionality, in addition to internet protocol (IP) address and other protocol-based restrictions. HMA also implements uniform resource locator (URL) and domain name system (DNS) filtering on all computers and servers. HMA regularly scans all systems to ensure vulnerabilities are quickly discovered and remediated. HMA adheres to internal patch management and change control policies. Penetration tests, HIPAA risk assessments and complete failover testing are performed annually.

Data Security

All HMA electronic data related to our projects are stored within folders that are accessible and visible to project team members only. All sensitive data is granted access on a "least privilege" principal. When necessary, electronic data and correspondence can be encrypted to provide greater security when transmitting sensitive data. To aid in secure communications, HMA also utilizes security appliances to automatically encrypt sensitive data. All project-related data is backed up nightly and is available off-site.

Data Transmission

HMA provides several methods for securely transmitting and receiving data to and from external resources. HMA uses SharePoint sites, with least privilege role-based access control (RBAC), to share larger files for longer periods of time. For smaller sets of data (too large for email) and shorter lengths of time (60 day maximum), HMA uses Proofpoint's Secure Share product for the secure exchange of large or sensitive files.

Data Integrity

HMA uses best practices in accordance with logging and event management to comply with any audit requests or regulatory requirements. Logs are sent to separate appliances to maintain the integrity of the data for compliance and forensic purposes. Servers, computers, and other networked nodes' logs are aggregated in a security information and event management (SIEM) appliance. HMA also utilizes a log aggregation appliance specifically for our firewalls.

Protected Health Information (PHI)

All HMA employees working with PHI have federal information processing standards (FIPS) compliant, self-encrypting hard drives and the ability to send or receive emails using advanced encryption standard (AES) 256-bit encryption. The information technology (IT) staff work closely with project managers to ensure strict compliance to our "need to know" policy when accessing confidential information. All relevant PHI is deleted upon the completion of a project or per the terms of the business associate agreement (BAA).

Access Control

All users are provided with unique usernames and passwords are both rotated regularly and technically required to adhere to complexity requirements. As part of HMA's offboarding procedure access is removed upon separation. All HMA devices are password protected, with mandatory screen timeouts and mandated password changes at regular intervals. Access to the internal network externally requires multi-factor authentication via HMA's virtual private network (VPN). VPN is subject to session timeouts.

Security Awareness Training

Information security training is provided annually to all HMA employees. All employees and subcontractors sign security policies stating they are aware of HMA's rules concerning computer and information security and will comply with all HMA's Information Security Policies and Procedures. Information security training includes, but is not limited to Security Awareness, Health Insurance Portability and Accountability Act of 1996 (HIPAA), and Health Information Technology for Economic and Clinical Health (HITECH) Act content. Other trainings, such as payment card industry (PCI) or fraud, waste, and abuse (FWA) may be assigned based on an individual's roles or responsibilities.

Background Checks

Comprehensive background checks are performed for all new employees, post offer acceptance, for the following areas: past employment, education, criminal (local/state/federal), civil, and verification of licensures (if applicable). Background checks for criminal are also periodically conducted for current employees as may be required by a client contract.

HMA Security Contacts

Information Systems Security Officer
Joshua Henry
Information Security Administrator
jhenry@healthmanagement.com
517-482-9236

Privacy Officer
Bill Jones
IT Director
bjones@healthmanagement.com
517-482-9236