HMS Information Security Program

HMS maintains a secure processing environment. Through annual and as-necessary reviews of our policies and procedures as well as exercises designed to test our secure environment, we continually build our system for security. We handle all data according to strict protocols, document and maintain that information in a central database, and update it as necessary. All our data-handling protocols address data security in accordance with both state and Federal requirements.

Our Information Security Management System (ISMS), in accordance with our Information Security policies, contains administrative, technical, and physical safeguards to protect our information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of our company, violate individual privacy rights, and possibly constitute a criminal act.

Under the direction of the Chief Security Officer, our IT Services team has developed policies, standards, guidelines, and practices for securing company information and technology assets.

HMS’s CSO maintains our Data Security Plan as well as our Facility Security Plan, which contains procedures to safeguard all facilities, systems, and equipment used to store PHI against unauthorized physical access, tampering, and theft. The CSO reviews the plans every six months and incorporates any necessary updates regarding contingency operations, access control and validation, Physical Access Records, and maintenance.

The preservation and enhancement of our reputation depends in part on the way in which we manage both information and information systems. Laws such as HIPAA, the Sarbanes-Oxley Act, and ARRA serve as guidelines for our data security processes and procedures. The domains defined in the International Organization for Standardization (ISO) 27001/27002, HITRUST CSF, and COBIT security frameworks influenced our methodology.

As part of our Corporate Compliance program, we have implemented (and maintain) our services to meet standards mandated by the HIPAA Privacy Rule. Our HIPAA security-compliance methodology goes beyond the requirements of the HIPAA Security Rule; it serves as a roadmap to safeguard not just electronic Protected Health Information (PHI) but HMS information assets as a whole.

This document was forwarded to University Benefits from HMS in May 2018.