Maryland Health Care Commission

Management Service Organizations
State Designation Criteria

Draft

February 19, 2010

TABLE OF CONTENTS

Overview

The effective use of health information technology (health IT) can help improve health care quality, prevent medical errors, and reduce costs by delivering essential information at the point of care. Successful health IT requires two crucial components – widespread use of electronic health records (EHRs) and the ability to exchange health information privately and securely. While both are challenging projects conceptually, technologically, and economically, the implementation of EHRs pose special challenges. These challenges mostly relate to the cost of the software and maintaining systems that support the application. The integration of EHRs into a physician practice takes time and is influenced by technological constraints, costs, and different perceptions and expectations. Management service organizations (MSOs) have emerged as a way to address these challenges.

MSOs are considered a viable alternative to the traditional EHR client-server model where the technology is maintained at the provider site. These organizations are capable of supporting multiple EHR products at reduced costs through economies of scale and bulk purchasing. Technical support usually extends beyond the standard business hours and in some instances is available on a 24/7 basis. Data is safeguarded through a network operating center that, by design, ensures high quality and uninterrupted service. MSOs enable physicians to access a patient's record wherever access to the Internet exists. EHRs maintained outside of the physician practice enables physicians to focus on practicing medicine rather than dedicating staff to support the application.

On May 19, 2009, Governor Martin O'Malley signed House Bill 706, *Electronic Health Records – Regulation and Reimbursement*, into law. This law requires the Maryland Health Care Commission (MHCC) to designate one or more MSOs that offer EHRs throughout the state by October 2012. The MHCC plans to work closely with stakeholders to develop criteria for state designation that reflects best practices regarding privacy and security.

STATE DESIGNATION I: DESIGNATION PROCESS

State Designated MSOs will need to meet the objectives below to retain their State Designation status.

- The MSO must conduct an independent review of their State Designation every two years.
- The MSO must begin the re-designation process six (6) months before the designation status expires.
- The MSO must perform a self-assessment using the Criteria guidelines.
- The MSO must agree to a site visit if requested by the MHCC.
- The MSO must use an independent third party accrediting agency recognized by the MHCC for evaluation of the MSO.
- The MSO must receive final approval from the MHCC for State Designation.

STATE DESIGNATION II: PRIVACY AND CONFIDENTIALITY

State Designated MSOs must have in place the appropriate Health Insurance Portability and Accountability Act (HIPAA) policies and procedures to ensure the integrity and confidentiality of protected health information (PHI). These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of electronic information. The policies and procedures must protect an individual's interests by managing who has access to PHI. The specific HIPAA regulation is referenced when appropriate.

MEASURES TO ENSURE DATA PRIVACY AND CONFIDENTIALITY
45 CFR §§ 164.530(c)

- The MSO must have appropriate policies for administrative, technical, and physical safeguards.
- The MSO must have policies to protect against inappropriate disclosure of PHI.
- The MSO must have policies and procedures in place to ensure continuing compliance with data security policies, including secure methods of access to and transmission of data.
- The MSO must use PHI about individuals only as is necessary.
- The MSO must refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.
- The MSO must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it. 45 CFR §§ 164.312(a)(2)(iv) *[See also CMS Internet Security Policy]*.
- The MSO must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software. 45 CFR §§ 164.308(a)(5)(ii)(B)
- The MSO must maintain a list of all individuals, contractors, and business associates with access to electronic PHI.
- The MSO must have policies in place that prohibit individuals from storing unencrypted PHI on portable devices.
- The MSO must demonstrate that appropriate security is in place for wireless networks to protect the privacy of data during transmission and in storage.
- The MSO must demonstrate that configuration standards are in place that includes patch management for systems which store, transmit, or access electronic PHI, including workstations.
- The MSO must implement policies and procedures to ensure compliance with any applicable federal or state privacy and security requirements.

- The MSO must notify their customer(s) of any PHI breach immediately after the breach is discovered.

- The MSO must have policies and procedures to ensure that PHI is not stored nor transported in an insecure manner.

STATE DESIGNATION III: TECHNICAL PERFORMANCE

State Designated MSOs must provide assurances and have policies in place to ensure that authorized users are able to access patient records in a timely manner. Areas of technical performance include:

- Customer service inquiries
- System availability
- Compliance with industry standards
- Capacity monitoring
- Auditing
- Storage and retrieval
- Internet

CUSTOMER SERVICE INQUIRIES

- The MSO must have an acknowledgment system and a tracking system that documents response times and procedures that are appropriate for different levels of requests.
- The MSO must have the capability to acknowledge inquiries within three business hours.
- The MSO must respond with a plan of action to open inquiries within one business day.
- The MSO must have documented escalation procedures to follow the inquiry to completion.

SYSTEM AVAILABILITY

- The MSO must have minimum system availability and appropriate redundancy that assures system access for 99.999% of contracted and/or advertised hours. This requirement shall not preclude acts of God.
- The MSO must provide support 24 x 7 x 365.
- The MSO must provide practices with a schedule of all downtime at least one week prior to the actual downtime.

COMPLIANCE WITH INDUSTRY STANDARDS

- The MSO must maintain a current analysis of any federal or state privacy or security laws that the MSO reasonably believes apply to information stored or transmitted by the MSO (e.g., security breach notification laws). The MSO must have a plan to comply with any such laws.

CAPACITY MONITORING

- The MSO must have the ability to measure system capacity and have an ongoing monitoring capability developed for measuring that system capacity.

- The MSO must have a formal system capacity plan for handling peak load and expansion including a demonstration of 99.5% availability on communication exchange components per the advertised service level agreements. This requirement does not preclude acts of God.

AUDITING

- The MSO must provide a clear and accurate auditing mechanism.

STORAGE AND RETRIEVAL

- The MSO must have an off-site location that has a six-month minimum backup archive, storage, and retrieval of all data and adheres to all applicable Federal and State regulations.

- The MSO must annually test the backup restoration process for all customer data.

- The MSO must have, or show progress toward having, a seven-year back-up archive, storage, and regeneration capabilities.

- The MSO must have the ability to partition data into separate files that can either be aggregated for a multi-provider practice or separated for extraction by a single provider of that multi-provider practice.

- The MSO must designate a hot-site that can be operational within four (4) hours.

INTERNET

- The MSO must have a firewall configured to protect the system integrity.

- The MSO must ensure that internal databases cannot be modified directly through an external web site, unless made securely, by authenticated users and contain integrity checks. Otherwise, all modifications to databases are to be made first only to external databases (e.g. those kept on the web server) and integrity checks made on the external database prior to synchronization with any internal database.

- The MSO must provide capacity and bandwidth adequate for business needs. The MSO must have a process in place to daily monitor Internet bandwidth and communication server performance.

- The MSO must have in place processes and procedures to monitor and/or block intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.

- The MSO must have documented procedures to respond to a successful intrusion or attack from the Internet within two (2) hours of when an alarm is generated or notification received.

- The MSO must have an established plan to conduct threat and vulnerability assessments through an independent third party. The MSO must develop an improvement process based on the results of those assessments.

- The MSO must have documented web server security configurations to protect the web server from attack or intrusion.

STATE DESIGNATION IV: BUSINESS PRACTICES

State Designated MSOs must have business practices that facilitate the maintenance of the Technical Performance Criteria and must exhibit truth-in-advertising (i.e., the MSO must actually do what it says it will do for customers). To qualify in this Criteria area, State Designated MSOs must: have procedures for measuring customer satisfaction; provide non-restricted systems of access; adequately provide for customer education and training; and have standard contracts or service agreements.

TRUTH-IN-ADVERTISING

- The MSO must meet their published service levels.
- The MSO must have policies and procedures to assure that any re-marketing agreements do not endanger compliance with the MSO State Designation Criteria.
- The MSO must conduct annual customer satisfaction surveys.

ACCESS

- The MSO must offer at least one nationally certified hosted EHR product.

AGREEMENTS

- The MSO must have service level agreements with all participating provider practices.
- The MSO must have a termination clause that allows a practice to terminate the agreement without cause or without reason within 90 days of entering into a contract.
- The MSO must agree to make the data available upon termination in a format requested by the provider.

STATE DESIGNATION V: RESOURCES

State Designated MSOs must possess the physical, human, and administrative resources necessary to maintain a high level of technical performance and business practices. These resources must include: facilities adequate to conduct the MSOs current and anticipated business volume and qualified staff.

PHYSICAL RESOURCES

- The MSO must have physical resources adequate for accomplishing the stated mission.
- The MSO must have formal facility expansion plans in place in anticipation of increased growth.

PERSONNEL

- The MSO must have sufficient, qualified personnel to perform all tasks associated with accomplishing the stated mission.
- The MSO must ensure that employees receive effective, relevant job training to remain current in knowledge and skills.
- The MSO must provide, at a minimum, annual job training that includes privacy, confidentiality, and security for all employees and contractors.
- The MSO must maintain a record of employee and contractor compliance with the routine training. A copy of the curriculum, and any versioning, must also be kept on file.

STATE DESIGNATION VI: SECURITY

State Designated MSOs must have appropriate administrative, technical, and physical safeguard policies and procedures to ensure the integrity and confidentiality of PHI. These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of the data

State Designated MSOs must comply with the applicable standards, implementation specifications, and requirements of the HIPAA Security Rule with respect to PHI. State Designated MSOs must:

- Ensure the confidentiality, integrity, and availability of all PHI that the company creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule;
- Ensure compliance with the HIPAA Security Rule by its workforce;
- Implement procedures to identify what individual state health care security statutes and rules may have application; conduct a gap analysis with HIPAA's Security Rules and deploy the necessary systems to ensure compliance; and
- Conduct a gap analysis with HIPAA Security Rules and deploy the necessary systems to ensure compliance.

ADMINISTRATIVE SAFEGUARDS

- The MSO must comply with all Federal and State security rules.
- The MSO must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the MSO.
- The MSO must implement an enforcement policy that will authorize the MSO to apply appropriate sanctions against workforce members (i.e., employees, contractors, and vendors) who are not in compliance with the MSO's security policies and procedures.
- The MSO must implement procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports and maintain/report discrepancies to the security officer for review.
- The MSO must implement policies and procedures to ensure that all members of the MSO's workforce have access only to PHI necessary to perform their work assignment and to prevent access to those workforce members who do not have a need to access electronic PHI.

- The MSO must implement termination procedures for withdrawing access to PHI when the employment of a workforce member ends.

- The MSO must implement and document a security awareness and training program for all members of the MSO's workforce.

- The MSO must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.

- The MSO must have a process in place to identify and respond to suspected or known security incidents; mitigate harmful effects of security incidents that are known to the MSO.

- The MSO must establish written policies and procedures for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that impacts systems that contain PHI.

- The MSO must include in their disaster recovery/business continuity plan the following: that the plan is tested annually, what constitutes a disaster, a communication plan notifying provider practices of the disaster and escalation process, and identification of critical personnel who are responsible for conducting the damage assessment and mitigation process.

- The MSO must implement and document procedures for periodic testing, assessment, and review and revision of contingency plans. Testing and all appropriate revisions should occur no less than annually.

PHYSICAL SAFEGUARDS

- The MSO must implement and document policies and procedures to limit physical access to its information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access.

- The MSO must establish procedures that allow secure facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

- The MSO must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
  45 CFR §§ 164.310(a)(2)(ii)

- The MSO must implement procedures to control and validate a person's access to data based on their role or function.

- The MSO must implement policies and procedures, including a log, governing the receipt and removal of hardware and electronic media that contain PHI into and out of a facility, and the movement of these items within the facility.

- The MSO must implement policies and procedures to address the final disposition of PHI and the hardware or electronic media on which it is stored.

- The MSO must implement procedures for removal of PHI from electronic media before the media are made available for re-use.

TECHNICAL SAFEGUARDS

- The MSO must implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.

- The MSO must assign a unique name and/or number for identifying and tracking all system user identities.

- The MSO must establish procedures for accessing necessary PHI during an emergency.

- The MSO must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

- The MSO must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.

ORGANIZATIONAL REQUIREMENTS FOR BUSINESS ASSOCIATE CONTRACTS

- The MSO must require Business Associates to implement administrative, physical, and technical policies and procedures that are reasonable, appropriate, and required by Federal and State Law to protect the confidentiality, integrity, and availability of the PHI it creates, receives, maintains, or transmits on behalf of the MSO.

- The MSO must require Business Associates to report to the MSO any security incident of which it becomes aware. 45 CFR §§ 164.314(a)(2)(i)(C)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

- The MSO must record and maintain the policies and procedures implemented to comply with applicable Federal and State regulations, and policies and procedures should be available to those that need access to them.

- The MSO must review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of the PHI.

STATE DESIGNATION VII: MEANINGFUL USE

A key function of the State Designated MSO is to provide implementation support, technical assistance, and ongoing assistance to practices to meet the meaningful use requirements.

- The MSO must conduct an operational assessment of physician practices for workflow and process improvements.

- The MSO must provide practice with written recommendations to practice on workflow redesign within 30 days of an operational assessment.

- The MSO must provide education to the practice and support where appropriate in their effort to become meaningful users of EHRs.

STATE DESIGNATION VIII: PERFORMANCE MEASURES

The State Designated MSO will provide performance measures on an annual basis and provide each practice with monthly reports.

- The MSO must conduct an annual provider satisfaction survey including measures on service offerings available to the practice, the functional use of the EHR to measure meaningful use adoption, and questions pertaining to support offerings including training, educational assistance, technical assistance and problem resolution.

- The MSO must publish an annual report to share with the Regional Extension Center (REC), the MHCC, and practices on the results of the provider satisfaction survey.

- The MSO must report on a quarterly basis the customer service numbers and resolution times based on the severity level of problems to the practices, REC, and the MHCC.

- The MSO must report annually the number of practices who have implemented EHRs to the REC and the MHCC.

- The MSO must use the REC established quality indicators to measure each practice and report quarterly to the practice, REC, and the MHCC.

STATE DESIGNATION IX: COLLABORATION WITH REGIONAL EXTENSION CENTERS (REC)

The State Designated MSO will work collaboratively with the REC to increase the adoption of EHRs.

- The MSO must support the REC as it relates to EHR education, awareness, and on-site support for practices.

- The MSO must agree to support the REC as it completes activities required by the Office of the National Coordinator for Health Information Technology and the MHCC.