Maryland Health Care Commission

Management Service Organizations
State Designation Criteria

Table of Contents

OVERVIEW

Utilizing health information technology (health IT) in an optimal manner 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 poses 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 offer centralized administrative and hosted technology services and are considered a viable alternative to the traditional EHR client-server model where the technology is maintained locally at the provider site. MSOs enable physicians to access patient records wherever access to the Internet exists. 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. Remotely hosted EHRs enable providers to focus on practicing medicine rather than dedicating staff to support the application and technology.

On May 19, 2009, Governor Martin O'Malley signed into law House Bill 706, *Electronic Health Records – Regulation and Reimbursement*. 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 convened an MSO Advisory Panel that developed the criteria for *State Designation*. The criteria outline the requirements for *MSO State Designation* and assess privacy and confidentiality, technical performance, business practices, resources, security, and operations of MSOs.

STATE DESIGNATION I: QUALIFYING EVENTS

MSOs will need to conform to select requirements in order to be considered for State Designation. The requirements and the Criteria are subject to change and existing State Designated MSOs that seek to renew their State Designation must meet the requirements in existence at the time of application.

- The MSO must offer a hosted EHR solution that is certified by a nationally recognized certifying organization.

- The MSO must complete an application and self-assessment manuscript using the Criteria recognized by the MHCC.

- The MSO and any subcontractor must provide services (i.e., education, technology, support, etc.) using a workforce where at least 50 percent of the resources originate in Maryland.

- The MSO must establish and maintain an active connection to the state designated health information exchange.

- The MSO must agree to a bi-annual site visit.

- The MSO must re-apply every two years and meet the requirements outlined in the MSO State Designation Criteria.

- The MSO must support state efforts and the efforts of the state designated health information exchange in advancing health information technology consistent with the goals of the Office of the National Coordinator for Health Information Technology.

STATE DESIGNATION II: PRIVACY AND CONFIDENTIALITY

State Designated MSOs must have appropriate policies and procedures in place that comply with the *Health Insurance Portability and Accountability Act of 1996* (HIPAA) requirements 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 also protect an individual's interests by managing who has access to PHI. The measures stated below reference specific information that should be discussed in the self-assessment manuscript.

MEASURES TO ENSURE DATA PRIVACY AND CONFIDENTIALITY

- 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 standards, including secure methods of access to and transmission of data.
- The MSO must refrain from selling, marketing or otherwise using PHI in any way that violates 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 federal or state legislation.
- The MSO must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software and/or intrusion events.
- The MSO must maintain a list of all individuals, contractors, and business associates with access to electronic PHI maintained by the MSO.
- The MSO must demonstrate that configuration standards are in place and include patch management for systems that store, transmit, or access electronic PHI, including workstations within the MSO.
- The MSO must implement policies and procedures to ensure compliance with any applicable federal and state privacy and security requirements.
- The MSO must notify their customer(s) in writing within 60 calendar days of discovering a breach or disclosure of PHI.
- The MSO must have policies and procedures to ensure that PHI is not stored nor transported in an insecure manner as established by federal and state security requirements.

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 health records in a timely manner. Areas of technical performance include:

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

CUSTOMER SERVICE INQUIRIES

- The MSO must have a service inquiry management and a tracking system that documents date and time of initial contact through resolution.
- The MSO must have the capability to acknowledge inquiries within three business hours.
- The MSO must respond to open inquiries within one business day with either a resolution or plan of action for issues requiring escalation.
- The MSO must have documented escalation procedures based on severity to follow the inquiry to completion.

SYSTEM AVAILABILITY

- The MSO must have minimum system availability and appropriate redundancy that assures system access for 98 percent of contracted and/or advertised hours. This requirement shall not preclude acts of nature.
- The MSO must support extended hours of support, if required by clients.
- The MSO must provide practices with a notice of all scheduled downtime at least one business week prior to the actual downtime.
- The MSO must notify all practices within two hours in the event of unscheduled downtime.

COMPLIANCE WITH INDUSTRY STANDARDS

- The MSO must maintain a current analysis of any federal and 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), and 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 in place for measuring that system and managing capacity.

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

AUDITING

- The MSO must implement an accurate and transparent 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 practice data.

- The MSO must have, or show progress towards having, a seven-year back-up archive, storage and regeneration capabilities at minimum, and a process for providing extended back-ups at the request of the practice.

- 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 have a process in place to have operations restored in a timely manner.

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 website, unless made securely, by authenticated users and contain integrity checks.

- The MSO must ensure that integrity checks are made on all modifications to external systems (e.g., those kept on the web server) 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 processes and procedures in place 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 a timely manner of when an alarm is generated or notification received.

- The MSO must have an established plan to conduct an annual threat and vulnerability assessment 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 sound business practices that support the goals of the organization. These business practices center on procedures for measuring customer satisfaction; provide non-restricted access to the system based on assigned level of access; adequately provide for customer education and training; and have standard contracts and service agreements.

TRUTH-IN-ADVERTISING

- The MSO must demonstrate compliance with their published service levels.

ACCESS

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

AGREEMENTS

- The MSO must have service level agreements that take into consideration the needs of the MSO and practice, and have reasonable termination provisions for both parties.

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 maintain qualified staff.

PHYSICAL RESOURCES

- The MSO must have physical resources adequate for accomplishing the stated mission.
- The MSO must regularly monitor capacity to support its defined services.
- The MSO must have a formal expansion plan in place when strategic plans project organizational growth of more than 10 percent annually.

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 training applicable with the HIPAA provisions for all employees and ensure contractors have received similar training.
- 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.
- The MSO must demonstrate a thorough due diligence process in their hiring practices.

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. MSOs must comply with all the HIPAA requirements. MSOs should uniquely describe their policies in the self-assessment manuscript relating to the following:

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.
- The MSO must maintain a record of any discrepancies noted from the record review and report these 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 to the minimum necessary PHI to perform work assignments and to prevent access to workforce members who do not need 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 and 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 impact systems that contain PHI.

- The MSO must include in their disaster recovery/business continuity plan the following: annual testing of the plan, what constitutes a disaster, a communication plan notifying providers 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 must 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.

- 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 discarded or 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 regulations 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.

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; 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: OPERATIONS

State Designated MSOs are required to support the activities of the Regional Extension Center. The leading areas of support center on EHR implementation support, technical assistance, and ongoing assistance to the provider to meet the *meaningful use* requirements established by the Centers for Medicare & Medicaid Services.

- The MSO must have an EHR adoption education plan for providers without an EHR system.

- The MSO must have a plan for maximizing EHR functionality of providers with an EHR system.

- The MSO must have a plan in place to furnish technical assistance to the providers participating with the MSO.

- The MSO must conduct an annual provider satisfaction survey under the guidance of the Regional Extension Center and in consultation with the MHCC and report on the findings.

APPENDIX

Acknowledgements

The Maryland Health Care Commission greatly appreciates the contribution made by everyone that participated in the Advisory Panel and the ongoing support in developing the criteria for state designation. Special thanks go to the following individuals for giving of their time to complete the designation criteria. The information provided by these individuals has led to this groundbreaking initiative.

Doug Abel
Anne Arundel Medical Center

Ray Adkins
Peninsula Regional Medical Center

Scott Afzal
Audacious Inquiry

Salliann Alborn
Community Health Integrated Partnership

Jama Allers
The Maryland State Medical Society

Karen Barker
LifeBridge Health

Lee Barrett
EHNAC

Shelby Boggs
NextGen Healthcare

Gary Broadwater
Antietam Health Services

Jeffrey Cheng
GURU Consulting

Chuck Dorin
e-MDs

Kathryn Feldmann
CGI System Integrators

Mike Fierro
Dynamed

Marty Frygier
Perficient

Beverly Gazmen
Chesapeake Ortho & Sports

Ed Grogan
Calvert Memorial

Chuck Henck
University Physicians, Inc

Michael Hill
SysInformation

David Horrocks
CRISP

Clay House
CareFirst

Scott Inter
Calvert Memorial

Steve Johnson
MedChi

Mary Jane Kamps
Union Hospital of Cecil County

Jennifer King
Solomon Eye Physicians

Barbara Klein
Concordant

Traci La Valle
Maryland Hospital Association

Darren Lacy
Johns Hopkins

Bel Leong-Hong
Knowledge Advantage

Ron Moser
EHNAC

Minh Nguyen
Millennium Enterprise

Dave Palmisano
Sandlot

David Quirke
Frederick Memorial Hospital

Denise Reeser
New Heights Consulting

Ewart Russell
Children's Pediatric Associates

Telly Shackleford
Sandlot

Michael Snyder
Planned Systems International

Matthew Tan
Knowledge Advantage

Kevin Tyler
Mid-Atlantic Systems

Tina Whims
Frederick Health Services

Gary White
Practice Works Systems