

**ELECTRONIC HEALTHCARE NETWORK
ACCREDITATION COMMISSION
(EHNAC)**

**Healthcare
Management Service Organization
Accreditation Program
(MSOAP)**

**For The
HEALTHCARE INDUSTRY**

*Version 1.1
Released: January 2012*

Lee Barrett, Executive Director

**For additional information see the EHNAC Web Site
<http://www.EHNAC.org/>**

© Copyright 2012 Electronic Healthcare Network Accreditation Commission (EHNAC). All rights reserved.

Prefatory Notes:

If a criterion is marked with [MANDATORY] it must be addressed in the self assessment. Any MANDATORY criteria that are not fully completed will cause the candidate to FAIL the entire site review.

Please refer to EHNAC's [Glossary of Terms](#) for definitions of any unfamiliar terms referenced throughout this document. The Glossary of Terms is located at the EHNAC web site, www.ehnac.org.

Site Review Note: EHNAC realizes that some of the supporting documentation might not be able to be included in the Self assessment for many reasons. If you deem this to be the case, clearly indicate what your supporting documentation is, why you are not including it in your self assessment and how you will demonstrate it during the on-site review with the site reviewer. Please note that your organization may need to compensate EHNAC for an additional site visit, if the time required to review the documents exceeds one day.

SECTION I: INTRODUCTION TO CANDIDATE ENVIRONMENT

Accredited companies must provide a diagram or a spreadsheet identifying where the organization's PHI is stored, received, maintained or transmitted.

I. A. PHI Flow

[I.A.1](#) **[MANDATORY]** Candidate must provide a diagram or spreadsheet listing all Essential Function sites including their name, address, relationship to the entity under review, and the functions performed.
{493}

SECTION II: 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.

II. A. Qualifying Events

- [II.A.1](#) [MANDATORY] Candidate must offer an EHR solution that is certified by an Office of the National Coordinator for Health Information Technology (ONC) Authorized Testing and Certification Body (ATCB).
{503}
- [II.A.2](#) The offered solution(s) must be hosted by Candidate or Candidate must have a master's services agreement with an application service provider (ASP)/SaaS solution that is certified by a nationally recognized certifying organization.
{504}
- [II.A.3](#) [MANDATORY] Candidate must complete an application and self-assessment manuscript using the Criteria recognized by the state in which the candidate operates.
{403}
- [II.A.4](#) [MANDATORY] Candidate and any subcontractor must provide services (i.e., education, technology, support, etc.) using a workforce where at least 60 percent of the resources originate in the state for which services are provided.
{505}
- [II.A.5](#) [MANDATORY] Candidate must include a plan for establishing and maintaining an active connection to the state designated health information exchange as part of the application process.
{506}
- [II.A.6](#) [MANDATORY] Candidate must demonstrate an active connection to the state designated health information exchange for its clients/providers as part of the re-application process.
{507}
- [II.A.7](#) [MANDATORY] Candidate must re-apply every two years and meet the requirements outlined in the MSO State Designation Criteria.
{407}
- [II.A.8](#) [MANDATORY] Candidate must provide evidence to assure that criteria implemented by a third party are consistent with established criteria.
{508}

SECTION III: PRIVACY AND CONFIDENTIALITY

Accredited companies must have appropriate administrative, technical and physical policies and procedures to ensure the integrity and confidentiality of protected healthcare information. These policies and procedures must protect against any anticipated threats or hazards to the security or integrity of such information. As a practical matter, the required level of security is intended to be commensurate with the attendant risks.

III. A. Privacy and Confidentiality

[III.A.1](#) [MANDATORY] Candidate must have policies to protect against inappropriate disclosure of PHI to ensure compliance with any applicable federal and state privacy and security requirements.
{509} 45 CFR §§ 164.530(c)

[III.A.2](#) [MANDATORY] Candidate 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.
{178}

[III.A.3](#) [MANDATORY] Candidate must refrain from selling, reselling, marketing or otherwise using PHI in any way that violates privacy or confidentiality.
{510} 45 CFR §§ 164.530(c)

[III.A.4](#) [MANDATORY] Candidate must utilize strong encryption, user authentication, message integrity, and support for non-repudiation as security measures in compliance with any legislation requiring it.
{450} HITECH § 13402(h); 45 C.F.R. §§ 164.312(a)(2)(iv), 164.312 (e)(2)(ii)

[III.A.5](#) [MANDATORY] Candidate must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software and/or intrusion events.
{511} 45 CFR §§ 164.308(a)(5)(ii)(B)

[III.A.6](#) [MANDATORY] Candidate must maintain a list of all individuals, contractors, and business associates with access to Electronic PHI.
{409} 45 CFR §§ 164.530(c)

[III.A.7](#) [MANDATORY] Candidate must demonstrate that configuration standards are in place that include patch management for systems which store, transmit, or access Electronic PHI, including workstations.
{186}

[III.A.8](#) [MANDATORY] Candidate must notify their customer(s) in writing within 60 calendar days of discovering a breach or disclosure of PHI.
{417}

[III.A.9](#) [MANDATORY] Candidate must have policies and procedures to ensure that PHI is not stored nor transported in an unsecure manner as established by federal and state security requirements.
{512}

[III.A.10](#) Candidate must demonstrate that configuration standards are in place that include patch management for systems which store, transmit, or access Electronic PHI, including workstations.
{186}

III. B. Compliance with Industry Standards

[III.B.1](#) Candidate must maintain a current analysis of any federal or state privacy or security laws that Candidate reasonably believes apply to information stored or transmitted by Candidate (e.g., security breach notification laws). Candidate must have a plan to comply with any such laws.
{210} 45 C.F.R. § 162

SECTION IV: TECHNICAL PERFORMANCE

Accredited companies must provide their customers with the capability to communicate messages and records electronically (e.g. Electronic Data Interchange) through compliance with the technical performance criteria in this section.

IV. A. Customer Service Inquiries

[IV.A.1](#) [MANDATORY] Candidate must have a service inquiry management and a tracking system that documents date and time of initial contact through resolution.
{513}

[IV.A.2](#) Candidate must have the capability to acknowledge inquiries within three business hours.
{515}

[IV.A.3](#) Candidate must respond to open inquiries within one business day with either a resolution or plan of action for issues requiring escalation.
{516}

[IV.A.4](#) Candidate must have documented escalation procedures based on severity to follow the inquiry to completion.
{517}

IV. B. System Availability

[IV.B.1](#) [MANDATORY] Candidate 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.
{518}

[IV.B.2](#) Candidate must support extended hours of support, if required by clients.
{424}

[IV.B.3](#) [MANDATORY] Candidate must provide practices with a notice of all scheduled downtime at least one business week prior to the actual downtime.
{425}

[IV.B.4](#) [MANDATORY] Candidate must notify all practices within two hours in the event of unscheduled downtime.
{426}

IV. C. Capacity Monitoring and Management

[IV.C.1](#) Candidate must have the ability to measure system capacity and have an ongoing monitoring capability in place for measuring that system and managing capacity.
{519}

[IV.C.2](#) Candidate must have a formal system capacity plan for handling load and expansion including a demonstration of 98 percent availability as per the advertised Service Level Agreements. This requirement does not preclude acts of nature.
{520}

IV. D. Storage and Retrieval

[IV.D.1](#) **[MANDATORY]** Candidate must have a secure alternate location that has a six-month minimum backup archive, storage and retrieval of all data, and adheres to all applicable federal and state regulations.
{521}

[IV.D.2](#) Candidate must demonstrate a successful initial test and annually test the full backup restoration process for all data of a single practice.
{522}

[IV.D.3](#) Candidate 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.
{433}

[IV.D.4](#) Candidate 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.
{434}

[IV.D.5](#) **[MANDATORY]** Candidate must have a process in place to have data restored within eight (8) business hours, consistent with an established Service Level Agreement.
{523}

[IV.D.6](#) Candidate must provide evidence that back-ups occur on a daily basis.
{524}

[IV.D.7](#) Candidate must implement processes to track and trouble-shoot data loss as a result of an application error, network outage, or other service disruption.
{525}

IV. E. Network and Related Safeguards

[IV.E.1](#) **[MANDATORY]** Candidate must demonstrate the adequacy of a firewall configured to protect the system integrity and auditing and have processes and procedures in place to monitor, block, and appropriately respond to intrusion attempts or attacks from the Internet and provide alarms to appropriate personnel.
{526}

[IV.E.2](#) **[MANDATORY]** Candidate 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 are to be made on the external database prior to synchronization with any internal database.
{222}

[IV.E.3](#) Candidate must provide capacity and bandwidth adequate for business needs. Candidate must have a process in place to monitor Internet bandwidth and communication server performance daily.
{224}

[IV.E.4](#) Candidate must have an established plan to conduct an annual threat and vulnerability assessment through an independent third party. The candidate must develop an improvement process based on the results of those assessments.
{527}

[IV.E.5](#) Candidate must have documented web server security configurations to protect the web server from attack or intrusion.
{229}

[IV.E.6](#) Candidate 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.
{441}

SECTION V: BUSINESS PRACTICES

Accredited companies must have business practices that facilitate the maintenance of the technical performance Criteria and must exhibit truth-in-advertising -- i.e., the company must actually be doing what it says it will do for customers.

V. A. Truth in Advertising

[V.A.1](#) Candidate must demonstrate compliance with its published material, products, pricing, and services.
{528}

V. B. Business Evaluation

[V.B.1](#) Candidate must have an established mechanism to conduct periodic self evaluations of its business practices for the purpose of performance improvement.
{529}

V. C. Ethics

[V.C.1](#) Candidate must demonstrate high ethical business practices in all its transactions.
{530}

V. D. Agreements

[V.D.1](#) Candidate must have service level agreements that take into consideration the needs of the candidate and practice, and have reasonable termination provisions for both parties.
{446}

[V.D.2](#) **[MANDATORY]** The Candidate must provide each client with a Disclosure Statement that includes at a minimum the following key elements:

- Conflicts of interest;
- Experience, such as the length of time the MSO has been State Designated or in Candidacy Status; and
- A list of services offered by the MSO.

{531}

[V.D.3](#) **[MANDATORY]** The Candidate must provide each client with a Master Schedule that outlines at a minimum the MSO's fees, services, and agreement terms for the client transaction. All fees, services, and agreement terms must be fully disclosed.
{532}

SECTION VI: RESOURCES

Accredited companies must possess the physical, human and administrative resources necessary to maintain a high level of technical performance and business practices. These resources must include: plant and equipment facilities adequate to conduct the company's current and anticipated business volume; qualified professional and staff personnel; and professional development programs to keep up with changes in the industry. While resource-related Criteria are primarily expressed in terms of inputs, they are required because of their basic role as guarantors of effective outcome performance.

VI. A. Physical Resources

[VI.A.1](#) [MANDATORY] Candidate must have physical resources (including plant facilities and the relevant hardware and software) adequate for accomplishing the stated mission.
{235}

[VI.A.2](#) Candidate must regularly monitor capacity to support its defined services.
{448}

VI. B. Personnel

[VI.B.1](#) Candidate must have personnel qualified to perform all tasks associated with published services.
{533} 45 CFR §§ 164.308

[VI.B.2](#) Candidate must ensure that employees receive effective, relevant job training to remain current in knowledge and skills.
{451}

[VI.B.3](#) Candidate must demonstrate a thorough due diligence process in their hiring practices.
{454}

SECTION VII: SECURITY

Accredited companies must comply with the applicable standards, implementation specifications, and requirements of the HIPAA Security Rule with respect to Electronic Protected Health Information (PHI). When applicable to them, accredited companies must comply with state information security statutes and rules (e.g., security breach notification laws). Accredited companies must:

- Ensure the confidentiality, integrity, and availability of all Electronic 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; and
 - 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.

VII. A. Administrative Safeguards

- [VII.A.1](#) [MANDATORY] Candidate must comply with all federal and state security rules.
{455}
- [VII.A.2](#) [MANDATORY] Candidate must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of PHI held by the candidate.
{244} 45 C.F.R. § 164.308(a)(1)(ii)(A)
- [VII.A.3](#) [MANDATORY] Candidate must implement an enforcement policy that will authorize the candidate to apply appropriate sanctions against Workforce members' contractors, vendors and their employees who are not in compliance with the security policies and procedures of the candidate.
{245} 45 C.F.R. § 164.308(a)(1)(ii)(C)
- [VII.A.4](#) [MANDATORY] Candidate must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
{68} 45 CFR §§ 164.308(a)(1)(ii)(D)
- [VII.A.5](#) [MANDATORY] Candidate must maintain a record of any discrepancies noted from the record review and report these discrepancies to the security officer for review.
{459}
- [VII.A.6](#) [MANDATORY] Candidate must implement policies and procedures to ensure that all members of the Candidate'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.
{534} 45 CFR §§ 164.308(a)(3)

- [VII.A.7](#) [MANDATORY] Candidate must implement termination procedures for withdrawing access to Electronic PHI when the employment of a Workforce member ends, the Workforce member's duties no longer justify the need to access Electronic PHI, or as required by determinations made as specified in the previous criterion.
{545} 45 C.F.R. § 164.308(a)(3)(ii)(C)
- [VII.A.8](#) [MANDATORY] Candidate must implement and document a security awareness and training program for all members of the candidate's Workforce, including management.
{255} 45 C.F.R. § 164.308(a)(5)
- [VII.A.9](#) [MANDATORY] Candidate must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.
{257} 45 C.F.R. § 164.308(a)(5)(ii)(D)
- [VII.A.10](#) [MANDATORY] Candidate 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 candidate.
{464}
- [VII.A.11](#) [MANDATORY] Candidate 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 Electronic PHI.
{259} 45 C.F.R. § 164.308(a)(7)
- [VII.A.12](#) [MANDATORY] Candidate 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.
{466}
- [VII.A.13](#) [MANDATORY] Candidate 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.
{535} 45 CFR §§ 164.308(a)(7)(ii)(D)

VII. B. Physical Safeguards

- [VII.B.1](#) [MANDATORY] Candidate must implement and document policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while also providing that all properly authorized persons have adequate access.
{268} 45 C.F.R. § 164.310(a)(1)

- [VII.B.2](#) **[MANDATORY]** Candidate 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.
{269} 45 C.F.R. § 164.310(a)(2)(i)
- [VII.B.3](#) **[MANDATORY]** Candidate must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
{270} 45 C.F.R. § 164.310(a)(2)(ii)
- [VII.B.4](#) **[MANDATORY]** Candidate must implement procedures to control and validate a person's access to data based on their role or function.
{536} 45 CFR §§ 164.310(a)(2)(iii)
- [VII.B.5](#) **[MANDATORY]** Candidate must implement policies and procedures, including a log, governing the receipt and removal of hardware and electronic media that contain Electronic PHI into and out of a facility, and the movement of these items within the facility.
{274} 45 C.F.R. § 164.310(d)(1)
- [VII.B.6](#) **[MANDATORY]** Candidate must implement policies and procedures to address the final disposition of Electronic PHI and/or the hardware or electronic media on which it is stored.
{275} 45 C.F.R. § 164.310(d)(2)(i)
- [VII.B.7](#) **[MANDATORY]** Candidate must implement procedures for removal of Electronic PHI from electronic media before the media are made available for re-use.
{276} 45 C.F.R. § 164.310(d)(2)(ii)
- [VII.B.8](#) Candidate must have security and breach notification procedures in place in conformance with HIPAA and HITECH requirements. These procedures must require that the notifications are to be delivered without unreasonable delay.
{422} HITECH § 13402; 45 C.F.R. §§ 164.400-14

VII. C. Technical Safeguards

- [VII.C.1](#) **[MANDATORY]** Candidate 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.
{278} 45 C.F.R. § 164.312(a)(1)
- [VII.C.2](#) **[MANDATORY]** Candidate must assign a unique name and/or number for identifying and tracking all systems' user identity.
{279} 45 C.F.R. § 164.312(a)(2)(i)

[VII.C.3](#) [MANDATORY] Candidate must establish procedures for accessing necessary Electronic PHI during an emergency.
{280} 45 C.F.R. § 164.312(a)(2)(ii)

[VII.C.4](#) [MANDATORY] Candidate must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
{281} 45 C.F.R. § 164.312(a)(2)(iii)

[VII.C.5](#) [MANDATORY] Candidate must implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use Electronic PHI.
{282} 45 C.F.R. § 164.312(b)

VII. D. Organizational Requirements for Business Associate Contracts

[VII.D.1](#) [MANDATORY] Candidate 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 Electronic PHI it creates, receives, maintains, or transmits on behalf of the candidate.
{283} 45 C.F.R. § 164.314(a)(2)(i)(A)

[VII.D.2](#) [MANDATORY] Candidate must require Business Associates to report to the candidate any security incident of which it becomes aware.
{285} 45 C.F.R. § 164.314(a)(2)(i)(C)

[VII.D.3](#) Candidate must have business associate agreements in place with every organization that contracts with it for the purpose of exchanging or routinely accessing electronic PHI.
{495} HITECH §13408, 45 CFR § 164.502(e)(2)

VII. E. Policies and Procedures and Documentation Requirements

[VII.E.1](#) [MANDATORY] Candidate 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.
{291} 45 C.F.R. §§ 164.316(b)(1)(i), 164.316(b)(2)(ii)

[VII.E.2](#) [MANDATORY] Candidate must review documentation annually, and update as needed, in response to environmental or operational changes affecting the security of the Electronic PHI.
{294} 45 C.F.R. § 164.316(b)(2)(iii)

SECTION VIII: 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.

VIII. A. Operations

- [VIII.A.1](#) Candidate must have an EHR adoption education plan for providers without an EHR system.
{484}
- [VIII.A.2](#) **[MANDATORY]** Candidate must have a plan for maximizing EHR functionality of providers with an EHR system, including connecting with the state designated health information exchange and reporting to a public health authority.
{537}
- [VIII.A.3](#) Candidate must have a plan in place to furnish technical assistance to the providers participating with the MSO.
{486}
- [VIII.A.4](#) Candidate must provide evidence of documented and demonstrated strategies for practices to select, implement, and meaningfully use certified EHR technology.
{538}
- [VIII.A.5](#) Candidate must provide project management support for the EHR implementation process, including individualized coaching, consultation, troubleshooting, and other activities required to assure that the provider is able to assess and enhance organizational readiness for EHR implementation.
{539}
- [VIII.A.6](#) Candidate must help practices to understand and implement technology and workflow process redesign changes needed to attain meaningful use requirements.
{540}
- [VIII.A.7](#) Candidate must assess and remediate gaps in IT infrastructure, configure the software to meet practice needs.
{541}
- [VIII.A.8](#) **[MANDATORY]** Candidate must assist practice in obtaining meaningful use, ensure adequate software training for all staff, and track and adhere to implementation timelines.
{542}

- [VIII.A.9](#) Candidate must assist practices by reviewing the ongoing utilization of the EHRs, and providing appropriate feedback and support to improve utilization of features essential for meaningful use.
{543}
- [VIII.A.10](#) Candidate must assist practices with understanding federal and state reporting requirements and work with provider's EHR vendor(s) to gather the specific data in order to report.
{544}
- [VIII.A.11](#) Candidate must conduct an annual provider satisfaction survey under the guidance of the Regional Extension Center and in consultation with the state and report on the findings.
{487}