

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

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

**For The
HEALTHCARE INDUSTRY**

*Version 1.0
Released: January 2011*

Lee Barrett, Executive Director

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

© Copyright 2011 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: QUALIFYING EVENTS

Narrative Summary indicating how the evidence reflects compliance with Criteria I.

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.

I.A. Qualifying Events

- [I.A.1](#) Candidate must offer a hosted EHR solution that is certified by a nationally recognized certifying organization.
{402}
- [I.A.2](#) Candidate must complete an application and self-assessment manuscript using the Criteria recognized by the state in which the candidate operates.
{403}
- [I.A.3](#) Candidate 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 the candidate's state.
{404}
- [I.A.4](#) Candidate must establish and maintain an active connection to the state designated health information exchange.
{405}
- [I.A.5](#) Candidate must agree to a biennial site visit.
{406}
- [I.A.6](#) Candidate must re-apply every two years and meet the requirements outlined in the MSO State Designation Criteria.
{407}
- [I.A.7](#) Candidate 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.
{408}

SECTION II: PRIVACY AND CONFIDENTIALITY

Narrative Summary indicating how the evidence reflects compliance with Criteria II.

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.

II.A. Privacy and Confidentiality

- [II.A.1](#) Candidate must have policies to protect against disclosure of PHI.
{177}
- [II.A.2](#) 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}
- [II.A.3](#) Candidate must refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.
{180}
- [II.A.4](#) 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)
- [II.A.5](#) Candidate must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software.
{182} 45 C.F.R. § 164.308(a)(5)(ii)(B)
- [II.A.6](#) Candidate must maintain a list of all individuals, contractors, and business associates with access to Electronic PHI.
{409} 45 CFR §§ 164.530(c)
- [II.A.7](#) 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}
- [II.A.8](#) Candidate must implement policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.
{243}

[II.A.9](#) Candidate must notify their customer(s) in writing within 60 calendar days of discovering a breach or disclosure of PHI.
{417}

[II.A.10](#) Candidate must have policies and procedures to ensure documents containing PHI are neither stored nor transported in an insecure manner outside the secured environment.
{371}

SECTION III: TECHNICAL PERFORMANCE

Narrative Summary indicating how the evidence reflects compliance with Criteria III.

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.

III.A. Customer Service Inquiries

- [III.A.1](#) Candidate must have an acknowledgment system and a trading partner tracking system that documents response times and procedures that are appropriate to different levels of requests.
{195}
- [III.A.2](#) Candidate must be able to acknowledge trading partner inquiries within three business hours.
{196}
- [III.A.3](#) Candidate must respond with a plan of action to open trading partner inquiries within one business day.
{197}
- [III.A.4](#) Candidate must have documented escalation procedures to follow the inquiry to completion.
{199}

III.B. System Availability

- [III.B.1](#) Candidate must have a minimum system availability and appropriate redundancy that assures system access for 98.0% of contracted and/or advertised hours. This requirement shall not include outages due to acts of God.
{436}
- [III.B.2](#) Candidate must support extended hours of support, if required by clients.
{424}
- [III.B.3](#) Candidate must provide practices with a notice of all scheduled downtime at least one business week prior to the actual downtime.
{425}
- [III.B.4](#) Candidate must notify all practices within two hours in the event of unscheduled downtime.
{426}

III.C. Compliance with Industry Standards

[III.C.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

III.D. Capacity Monitoring and Management

[III.D.1](#) Candidate must have the ability to measure system capacity and have developed an on-going monitoring capability for that system capacity.
{214}

[III.D.2](#) Candidate must have a 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 include outages due to acts of God.
{429}

III.E. Auditing

[III.E.1](#) Candidate must implement an accurate and transparent auditing mechanism.
{430}

III.F. Storage and Retrieval

[III.F.1](#) Candidate must have an off-site minimum of six-month back-up archive, storage and retrieval capability for all batch transactions and adhere to all applicable federal and state regulations.
{415}

[III.F.2](#) Candidate must annually test the backup restoration process for all practice data.
{432}

[III.F.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}

[III.F.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}

[III.F.5](#) Candidate must have a process in place to have operations restored in a timely manner.
{435}

III.G. Internet Access

[III.G.1](#) Candidate must have a firewall configured to protect the system integrity.
{221}

[III.G.2](#) 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}

[III.G.3](#) Candidate 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.
{438}

[III.G.4](#) 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}

[III.G.5](#) Candidate 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.
{225}

[III.G.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}

[III.G.7](#) Candidate must on at least a quarterly basis conduct threat and vulnerability assessments and have an improvement process based on the results of those assessments. At least annually these assessments must be conducted through an independent third party.
{227}

[III.G.8](#) Candidate must have documented web server security configurations to protect the web server from attack or intrusion.
{229}

SECTION IV: BUSINESS PRACTICES

[Narrative Summary indicating how the evidence reflects compliance with Criteria IV.](#)

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.

IV.A. Truth-In-Advertising

[IV.A.1](#) Candidate must meet their own published service levels.
{231}

IV.B. Access

[IV.B.1](#) Candidate must offer at least one nationally certified hosted EHR solution.
{445}

IV.C. Agreements

[IV.C.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}

SECTION V: RESOURCES

Narrative Summary indicating how the evidence reflects compliance with Criteria V.

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.

V.A. Physical Resources

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

V.A.2 Candidate must regularly monitor capacity to support its defined services.
{448}

V.A.3 Candidate must have a formal expansion plan in place when strategic plans project organizational growth of more than 10 percent annually.
{449}

V.B. Personnel

V.B.1 Candidate must have sufficient qualified personnel to perform all tasks associated with accomplishment of the stated mission.
{237} 45 C.F.R. § 164.308

V.B.2 Candidate must ensure that employees receive effective, relevant job training to remain current in knowledge and skills.
{451}

V.B.3 Candidate must provide, at a minimum, annual job training, which includes breach reporting and notification, privacy, and confidentiality, and security for all employees and contractors with access to PHI.
{419} 45 C.F.R. § 164.308(a)(5)(i); HITECH § 13402

V.B.4 Candidate 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.
{453}

V.B.5 Candidate must demonstrate a thorough due diligence process in their hiring practices.

{454}

SECTION VI: SECURITY

Narrative Summary indicating how the evidence reflects compliance with Criteria VI.

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.

VI.A. Administrative Safeguards

[VI.A.1](#) Candidate must comply with all federal and state security rules.
{455}

[VI.A.2](#) 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)

[VI.A.3](#) 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)

[VI.A.4](#) 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)

[VI.A.5](#) Candidate must maintain a record of any discrepancies noted from the record review and report these discrepancies to the security officer for review.
{459}

[VI.A.6](#) Candidate must implement policies and procedures to ensure that all members of the candidate's Workforce have access only to Electronic 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.

{248} 45 C.F.R. § 164.308(a)(3)

[VI.A.7](#) 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 criterion V.B.6.
{250} 45 C.F.R. § 164.308(a)(3)(ii)(C)

[VI.A.8](#) 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)

[VI.A.9](#) 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)

[VI.A.10](#) 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}

[VI.A.11](#) 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)

[VI.A.12](#) 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}

[VI.A.13](#) Candidate must implement and document procedures for periodic testing, assessment, review and revision of contingency plans. Testing and all appropriate revisions should occur no less than annually.
{263} 45 C.F.R. § 164.308(a)(7)(ii)(D)

VI.B. Physical Safeguards

[VI.B.1](#) 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)

- [VI.B.2](#) 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)
- [VI.B.3](#) 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)
- [VI.B.4](#) Candidate must implement procedures to control and validate a person's access to facilities based on their role or function including visitor control and control of access to software programs for testing and revision.
{271} 45 C.F.R. § 164.310(a)(2)(iii)
- [VI.B.5](#) 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)
- [VI.B.6](#) 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)
- [VI.B.7](#) 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)
- [VI.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

VI.C. Technical Safeguards

- [VI.C.1](#) 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)
- [VI.C.2](#) 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)
- [VI.C.3](#) Candidate must establish procedures for accessing necessary Electronic PHI during an emergency.

{280} 45 C.F.R. § 164.312(a)(2)(ii)

[VI.C.4](#) 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)

[VI.C.5](#) 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)

VI.D. Organizational Requirements for Business Associate Contracts

[VI.D.1](#) 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)

[VI.D.2](#) 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)

[VI.D.3](#) Candidate must require that all Business Associates notify the Candidate in the event any PHI is improperly used or disclosed, including for the purpose of the breach notification rule.
{491} HITECH §13404(b), 45 CFR §§ 164.314(a)(2)(i)(C)

[VI.D.4](#) 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.
{492} HITECH §13408, 45 CFR § 164.502(e)(2)

VI.E. Policies and Procedures and Documentation Requirements

[VI.E.1](#) 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)

[VI.E.2](#) 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)

VI.E.3 Candidate must ensure Business Associates are contractually required to comply with all applicable Federal and State regulations including HITECH privacy and security requirements.
{423} HITECH §§ 13401(a), 13404(a)

SECTION VII: OPERATIONS

Narrative Summary indicating how the evidence reflects compliance with Criteria VII.

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.

VII.A. Operations

- VII.A.1 Candidate must have an EHR adoption education plan for providers without an EHR system.
{484}
- VII.A.2 Candidate must have a plan for maximizing EHR functionality of providers with an EHR system.
{485}
- VII.A.3 Candidate must have a plan in place to furnish technical assistance to the providers participating with the MSO.
{486}
- VII.A.4 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}