ELECTRONIC HEALTHCARE NETWORK ACCREDITATION COMMISSION (EHNAC)

HEALTH INFORMATION EXCHANGE ACCREDITATION PROGRAM (HIEAP) Criteria

For The

HEALTHCARE INDUSTRY

Version 1.0

Release Date: October 2010

Lee Barrett, Executive Director

For additional information see the EHNAC Web Site
www.EHNAC.org

© Copyright 2010 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.

Each criterion now includes its unique identifier from the EHNAC criteria database. This identifier immediately follows the text of each criterion and is enclosed in braces

{}. This identifier is helpful for comparing criteria between the various EHNAC programs and versions.

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.

CRITERIA I: 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.

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

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

I.A.1 **[MANDATORY]** Candidate must have policies to protect against disclosure of PHI.
{177}

I.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}

I.A.3 Candidate must limit the use, disclosure, or request of PHI, to the extent practicable, to a limited data set or, if needed, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request.
{437} HITECH §13405(b)(1)(A), 45 C.F.R. §164.502(b)

I.A.4 Candidate must refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.
{180}

I.A.5 **[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. Data sent or received through an unsecured network, including a wireless network, must be protected by NIST's FIPS 140-2 standards and using FIPS 140-2 compliant encryption software.
{450} HITECH § 13407 (h), 45 CFR 164.312(a)(2)(iv), 45 CFR 164.312 (e)(2)(ii)

I.A.6 Candidate must use effective controls and implement procedures for guarding against, detecting, and reporting malicious software.
{182} 45 CFR §§ 164.308(a)(5)(ii)(B)

I.A.7 **[MANDATORY]** Candidate must maintain a list of all individuals, contractors, and business associates with access to Electronic PHI.
{409} 45 CFR §§ 164.530(c)

I.A.8 **[MANDATORY]** Candidate must have policies in place that prohibit individuals from storing unencrypted PHI on personal computers, consumer devices, and removable storage media.
{410} 45 CFR §§ 164.530(c)

I.A.9 Candidate must demonstrate that appropriate security is in place for wireless networks to protect the privacy of data during transmission and in storage.
{185}

I.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}

I.A.11 Candidate must implement a security measure to ensure that electronically transmitted PHI is not improperly modified without detection.
{187} 45 CFR §§ 164.312(e)(2)(i)

I.A.12 Candidate must implement policies and procedures to ensure compliance with applicable requirements of the HIPAA Privacy and Security Rules.
{243}

CRITERIA II: TECHNICAL PERFORMANCE

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

II.A. TRANSMISSION OF DATA

II.A.1 **[MANDATORY]** Candidate must be able to receive and submit 100% of all eligible transactions electronically from and to all trading partners who accept or generate transactions electronically.
{191}

II.A.2 **[MANDATORY]** Candidate must be able to convert data to ensure interoperability as required by any service level agreements.
{411}

II.A.3 Candidate must make available real-time transactions and not impose limitations.
{428}

II.A.4 **[MANDATORY]** Candidate must comply with all applicable federal and state requirements and regulations.
{194}

II.B. TRADING PARTNER INQUIRIES

II.B.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}

II.B.2 Candidate must be able to acknowledge trading partner inquiries within three business hours.
{196}

II.B.3 Candidate must respond with a plan of action to open trading partner inquiries within one business day.
{197}

II.B.4 Candidate must respond with a plan of action to operational critical trading partner inquiries within four hours during normal business hours.
{198}

II.B.5 Candidate must have documented escalation procedures to follow the inquiry to completion.
{199}

II.C. TIMELINESS

II.C.1 Candidate must transmit 100% of all valid batch transactions and store and forward data within thirty minutes of receipt.
{201}

II.C.2 Candidate must process real-time transactions on an average of no longer than two seconds from the time any transaction is received until it is passed on to the next recipient.
{202}

II.D. DATA VALIDATION

II.D.1 Candidate must be able to demonstrate that 100% of transactions are either delivered successfully to the trading partner or are reported to the originator as undeliverable.
{203}

II.D.2 Candidate must provide for the monitoring and reporting of failed data transmissions to the sender. Reporting should specifically indicate the source of the problem for resolution if known.
{206}

II.E. SYSTEM AVAILABILITY

II.E.1 **[MANDATORY]** 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.
{412}

II.E.2 Candidate must notify trading partners regarding critical service outages outside the standard maintenance schedule prior to the planned outages.
{421}

II.F. COMPLIANCE WITH INDUSTRY STANDARDS
45 CFR §§ 162

II.F.1 Candidate must have the capability to support generally accepted industry standard formats and those required by federal and state regulations in a line of business as specified in the trading partner agreement.
{208}

II.F.2 **[MANDATORY]** Candidate must have an established implementation plan for compliance with all applicable federal and state adopted rules and implementation guides. This implementation plan should include at least an implementation sequence and timetable for implementation within mandatory timeframes.
{413} 45 CFR §§ 162

II.F.3 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.
{431}

II.G. CAPACITY MONITORING

II.G.1 Candidate must have the ability to measure system capacity and have developed an on-going monitoring capability for that system capacity.
{214}

II.G.2 Candidate 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 include outages due to acts of God.
{414}

II.H. AUDITING

II.H.1 Candidate must provide a clear and accurate audit trail permitting monitoring of all data transactions for a minimum of seven years.
{216}

II. I. Intentionally Left Blank

II.J. STORAGE AND RETRIEVAL

II.J.1 **[MANDATORY]** 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.
{217}

II.J.2 Candidate must have one-day storage and retrieval capability for real-time transactions.
{218}

II.K. INTERNET

II.K.1 **[MANDATORY]** Candidate must provide editing capabilities for all trading partners for administrative transactions.
{211}

II.K.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}

II.K.3 Candidate must authenticate the trading partner sending or receiving healthcare data.
{223}

II.K.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}

II.K.5 **[MANDATORY]** 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}

II.K.6 Candidate must have documented procedures to respond to a successful intrusion or attack from the Internet within 2 hours of alarm generation or notification.
{226}

II.K.7 **[MANDATORY]** 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}

II.K.8 Candidate must have documented procedures to check public security web sites, Web O/S vendor and web application vendors on at least a weekly basis to identify potential security weaknesses and update web server O/S and application configurations to eliminate or reduce those known weaknesses.
{228}

II.K.9 Candidate must have documented web server security configurations to protect the web server from attack or intrusion.
{229}

II.K.10 Candidate must not have any file transfer servers configured to reside on a firewall in such a manner that the file transfer server may be able to be accessed through a “port forwarding” configuration through the firewall.
{230}

CRITERIA III: BUSINESS PRACTICES

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

III.A. TRADING PARTNER AGREEMENTS

III.A.1 Candidate must meet their own published service levels.
{231}

III.A.2 Candidate must have policies and procedures to assure that any trading partner agreements do not endanger compliance with the EHNAC HIE Accreditation Criteria.
{301}

III.A.3 The HIE must have policies requiring periodic audits to monitor the use of the HIE to ensure compliance with applicable federal and state privacy law and HIE policies, and include the following in the audit:

- Consents are on file at the appropriate entity (HIE or trading partner) for patients whose PHI is accessed via the HIE; and

- HIE trading partner or business associate agreements require that authorized users who access PHI do so for authorized purposes.
{439}

III.A.4 The HIE must have policies requiring that the compliance audits are conducted at least once every twelve (12) months.
{440}

III.A.5 The HIE must have policies requiring auditing of adherence to privacy terms of HIE business associate agreements by all or a statistically significant subset of business associates.
{442}

III.B. ACCESS

III.B.1 Candidate must be capable of interconnecting to other HIEs via accepted message formats and transport protocols.
{443}

III.C. CONSUMER ENGAGEMENT

III.C.1 Candidate must demonstrate consumer engagement through their representation in advisory groups, educational materials, and a feedback mechanism from consumers used for continually improving communication and services.
{444}

III.C.2 Candidate must provide periodic and on-demand reports to consumers regarding HIE system performance, information access audit reports, and privacy violation notices.
{447}

III.D. RELATIONSHIPS WITH FEDERAL AND STATE GOVERNMENTS

III.D.1 Candidate must have developed or be in the process of developing the state HIE plan as defined by the Office of National Coordinator of Health Information Technology (ONCHIT) if selected as the State Designated Entity (SDE) by the governor of the state. If not the designated SDE, candidate must demonstrate formal relationships developed with the SDE for coordinating and accelerating HIE services within the state.
{452}

III.D.2 Candidates that plan to share information over the Nationwide Health Information Network (NHIN) must demonstrate that they have signed the documents required to be such a participant.
{456}

III.D.3 Candidate must comply with the functionality required under the Meaningful Use criteria (e.g., the ability to create a registry), and meeting the stipulated Meaningful Use schedule.
{457}

CRITERIA IV: RESOURCES

Narrative Summary indicating how the evidence reflects compliance with Standard IV.

IV.A. PHYSICAL RESOURCES

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

IV.A.2 Candidate must have formal facility expansion plans in place to anticipate increased growth. These plans should be reviewed regularly.
{236}

IV.B. PERSONNEL
45 CFR §§ 164.308

IV.B.1 Candidate must have sufficient qualified personnel to perform all tasks associated with accomplishment of the stated mission.
{237}

IV.B.2 Candidate must ensure that employees receive effective, relevant job training, and access to professional development opportunities necessary to remain current in knowledge and skills.
{238}

IV.B.3 **[MANDATORY]** 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 CFR §§ 164.308(a)(5)(i), HTIECH §13402(a)

IV.B.4 Candidate must maintain a list of individuals, down to the manager level, who are responsible for HIPAA compliance including the protection of Electronic PHI.
{458}

CRITERIA V: SECURITY

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

V.A. ORGANIZATIONAL REQUIREMENTS FOR HYBRID ENTITIES
45 CFR §§ 164.105

V.A.1 Candidate must have policies and procedures to ensure that its healthcare component protects PHI from another component within the candidate organization in accordance with the HIPAA Privacy and Security Rules.
{241}

V.A.2 Candidate must document the designated health care components of any Hybrid Entity in accordance with the Security Rule.
{242}

V.B. ADMINISTRATIVE SAFEGUARDS
45 CFR §§ 164.308

V.B.1 **[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 CFR §§ 164.308(a)(1)(ii)(A)

V.B.2 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 CFR §§ 164.308(a)(1)(ii)(C)

V.B.3 Candidate 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.
{246} 45 CFR §§ 164.308(a)(1)(ii)(D), 45 CFR §§ 164.308(a)(5)(ii)(C)

V.B.4 Candidate must identify the privacy official and the security official, and those persons' backups, that are responsible for the development, implementation and enforcement of the policies and procedures required by the Privacy and Security Rules. These responsibilities must be documented, including a description of their responsibilities, and communicated internally.
{247} 45 CFR §§ 164.308(a)(2)

V.B.5 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 CFR §§ 164.308(a)(3)

V.B.6 Candidate must implement procedures to determine that the access of a Workforce member, vendor, contractor and their employees to Electronic PHI is appropriate and is limited to only that which is necessary to the performance of work duties.
{249} 45 CFR §§ 164.308(a)(3)(ii)(B)

V.B.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 CFR §§ 164.308(a)(3)(ii)(C)

V.B.8 Candidate must implement appropriate administrative, technical, and physical safeguards to protect the privacy of PHI with the applicable requirements in the HIPAA Privacy Rule.
{251} 45 CFR §§ 164.530(c)

V.B.9 Candidate must, if acting as part of a larger organization, implement policies and procedures that protects and secures the electronic PHI handled by the candidate organization from unauthorized access by the larger organization as well as their employees, vendors and contractors.
{252} 45 CFR §§ 164.308(a)(4)(ii)(A)

V.B.10 Candidate and their contractors must maintain a listing of all hardware and software used to store, transmit or maintain Electronic PHI, including all Primary Domain Controllers (PDCs) and servers. Documentation must be provided showing which software resides on which hardware.
{253}

V.B.11 Candidate must implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
{254} 45 CFR §§ 164.308(a)(4)(ii)(B), 45 CFR §§ 164.308(a)(4)(ii)(C)

V.B.12 Candidate must implement and document periodic security updates, reminders and refresher programs for the members of the candidate's Workforce, including management.
{256} 45 CFR §§ 164.308(a)(5)(ii)(A)

V.B.13 Candidate must implement and document procedures for creating, changing, and safeguarding passwords and/or other login procedures.
{257} 45 CFR §§ 164.308(a)(5)(ii)(D)

V.B.14 **[MANDATORY]** Candidate 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 candidate or its Workforce; and appropriately document security incidents and their outcomes.
{258} 45 CFR §§ 164.308(a)(6)(ii)

V.B.15 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 CFR §§ 164.308(a)(7)

V.B.16 Candidate must establish and implement procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI if candidate stores PHI.
{260} 45 CFR §§ 164.308(a)(7)(ii)(A)

V.B.17 **[MANDATORY]** Candidate must establish and implement disaster recovery procedures to restore any loss of data, with the Recovery Point Objective not to exceed 48 hours and the Recovery Time Objective not to exceed 48 hours for critical transaction processing.
{261} 45 CFR §§ 164.308(a)(7)(ii)(B)

V.B.18 Candidate must establish, document, and implement emergency mode operations procedures to enable continued protection of the Electronic PHI.
{262} 45 CFR §§ 164.308(a)(7)(ii)(C)

V.B.19 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 CFR §§ 164.308(a)(7)(ii)(D)

V.B.20 Candidate must establish a process and perform an annual applications and data criticality analysis by assessing the relative criticality of specific applications and data in support of other contingency plan components.
{264} 45 CFR §§ 164.308(a)(7)(ii)(E)

V.B.21 Candidate must establish a process to continuously monitor and perform an annual technical and non-technical evaluation based on applicable Federal and State regulations and standards and subsequently respond to changes affecting the security of Electronic PHI that demonstrates the extent to which an entity's security policies and procedures meet the requirements of Federal and State regulations.
{265} 45 CFR §§ 164.308(a)(8)

V.B.22 Candidate must have Business Associate contracts in place that obtain satisfactory assurances that the Business Associate will uphold applicable Federal and State regulations.
{266} 45 CFR §§ 164.308(b)(1)

V.B.23 Candidate must have security and breach notification procedures in place in conformance with HIPAA and HITECH requirements.
{460}

V.C. PHYSICAL SAFEGUARDS
45 CFR §§ 164.310

V.C.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 CFR §§ 164.310(a)(1)

V.C.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 CFR §§ 164.310(a)(2)(i)

V.C.3 Candidate must implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
{270} 45 CFR §§ 164.310(a)(2)(ii)

V.C.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 CFR §§ 164.310(a)(2)(iii)

V.C.5 Candidate must implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security such as hardware, walls, doors, and locks.
{272} 45 CFR §§ 164.310(a)(2)(iv)

V.C.6 Candidate must implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access Electronic PHI.
{273} 45 CFR §§ 164.310(b)

V.C.7 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 CFR §§ 164.310(d)(1)

V.C.8 **[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 CFR §§ 164.310(d)(2)(i)

V.C.9 Candidate must implement procedures for removal of Electronic PHI from electronic media before the media are made available for re-use.
{276} 45 CFR §§ 164.310(d)(2)(ii)

V.C.10 **[MANDATORY]** Candidate must implement policies and procedures to address the final disposition of paper containing PHI, including the appropriate shredding and disposal of such documents.
{98}

V.C.11 Candidate must implement policies and procedures to create a retrievable exact copy of Electronic PHI before movement of equipment where PHI is stored.
{277} 45 CFR §§ 164.310(d)(2)(iv)

V.D. TECHNICAL SAFEGUARDS

V.D.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 CFR §§ 164.312(a)(1)

V.D.2 Candidate must assign a unique name and/or number for identifying and tracking all systems' user identity.
{279} 45 CFR §§ 164.312(a)(2)(i)

V.D.3 Candidate must establish procedures for accessing necessary Electronic PHI during an emergency.
{280} 45 CFR §§ 164.312(a)(2)(ii)

V.D.4 Candidate must implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
{281} 45 CFR §§ 164.312(a)(2)(iii)

V.D.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 CFR §§ 164.312(b)

V.E. ORGANIZATIONAL REQUIREMENTS FOR BUSINESS ASSOCIATE CONTRACTS
45 CFR §§ 164.308(b)(1)

V.E.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 CFR §§ 164.314(a)(2)(i)(A)

V.E.2 Candidate must require Business Associates to ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate policies and procedures to protect it.
{284} 45 CFR §§ 164.314(a)(2)(i)(B)

V.E.3 Candidate must require Business Associates to report to the candidate any security incident of which it becomes aware.
{285} 45 CFR §§ 164.314(a)(2)(i)©

V.E.4 Candidate must require Business Associates to authorize termination of the Business Associates' contract by the candidate, in the event candidate determines that the Business Associate has violated a material term of the contract.
{286} 45 CFR §§ 164.314(a)(2)(i)(D)

V.E.5 Candidate must ensure Business Associates are contractually required to comply with all applicable Federal and State regulations including HITECH privacy and security requirements.
{461}

V.E.6 The HIE must have policies that require each trading partner to enter into a business associate agreement with the HIE.
{415}

V.F. POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS

V.F.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 CFR §§ 164.316(b)(1)(i), 45 CFR §§ 164.316(b)(2)(ii)

V.F.2 Candidate must maintain a written and/or electronic record of any action, activity, or assessment that may be required by applicable Federal and State regulations.
{292} 45 CFR §§ 164.316(b)(1)(ii)

V.F.3 Candidate must retain the documentation, referred to herein, for 6 years from the date of creation or the date when it was last in effect, whichever is later.
{293} 45 CFR §§ 164.316(b)(2)(i)

V.F.4 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 CFR §§ 164.316(b)(2)(iii)

HIEAP PRIVACY & SECURITY POLICIES

PREFACE

The Electronic Healthcare Network Accreditation Commission (EHNAC) developed privacy and security policies for health information exchanges (HIEs). These policies identify a standard for privacy and security as it relates to consent, authorization, authentication, access, and audit. EHNAC recognizes the differences that will naturally exist among HIEs and these policies capture a broad sense of policies that HIEs may have or plan to implement. The policies outlined will be applicable if the HIE has adopted and integrated these policies into practice.

CRITERIA VI: CONSENT

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

The health information exchange (HIE) shall allow an authorized participant to access protected health information (PHI) if the patient has provided consent authorizing the participant access to the information.

VI.A. GENERAL

VI.A.1 The HIE must have a policy that specifies the approach to patient consent to participate in the HIE. (i.e., opt-in, opt-out, or no consent required).
{463}

VI.A.2 The HIE must have a policy that specifies the patient consent required to query their PHI.
{465}

VI.B. PUBLIC HEALTH REPORTING

VI.B.1 The HIE must have policies for the release of information to a government agency as mandated by law or as permitted by HIE policy.
{467}

VI.C.EMERGENCY TREATMENT

VI.C.1 The HIE must have policies that enable providers to access PHI in emergency situations in compliance with patient consent policies.
{468}

VI.C.2 The HIE must have policies that ensure that Emergency Treatment Disclosure access is terminated upon completion of the emergency treatment.
{469}

VI.D. MINORS

VI.D.1 The HIE must have policies regarding PHI for minors.
{470}

VI.E. CHANGE OF CONSENT

VI.E.1 The HIE must have policies that entitle patients to change consent at any time provided that such change does not preclude any PHI previously accessed by HIE trading partners.
{471}

CRITERIA VII: AUTHORIZATION

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

The HIE shall allow authorized users access to PHI based upon the role of that user in providing treatment, payment for treatment, and health care operations.

VII.A. CATEGORIES OF AUTHORIZED USERS

VII.A.1 The HIE must have policies that describe its user authorization process. (includes all trading partners/users in the HIE).
{472}

VII.B. PURPOSE OF ACCESS

VII.B.1 The HIE must have policies that restrict the role-based access to the HIE based on authorized user's employment responsibilities.
{473}

VII.B.2 The HIE must have policies that require that the authorized user who accesses PHI through the candidate's systems to attest to the purpose of their access every time data is accessed.
{474}

CRITERIA VIII: AUTHENTICATION

Narrative Summary indicating how the evidence reflects compliance with Standard VIII.

The HIE shall require participants to pass an authentication methodology prior to receiving access to PHI.

VIII.A. PROOF OF IDENTITY

VIII.A.1 The HIE must have policies that require the HIE, or trading partner entities, to verify proof of identity for their authorized users upon application for access to the HIE.
{475}

VIII.B. AUTHENTICATION DATA

VIII.B.1 The HIE must have policies that ensure the following:
- Authentication data is secure as it is entered;
- Authentication data is administered properly;
- Authentication actions are recorded corresponding to unique users; and
- Security of active and non-active user IDs and passwords.

{476}

CRITERIA IX: ACCESS

Narrative Summary indicating how the evidence reflects compliance with Standard IX.

The HIE shall allow authorized users to have access to only the PHI consistent with patient consent.

IX.A. AUTHORIZED PURPOSES

IX.A.1 The HIE must have policies that permit authorized users to access PHI only for the purposes consistent with the patient's consent status or as permitted by HIPAA, and state and federal law.
{477}

IX.B. RECORD LOCATOR SERVICE AND OTHER COMPARABLE DIRECTORIES

IX.B.1 If record locator services are provided by the HIE then policies must be in place for those services that implement reasonable safeguards to minimize unauthorized incidental disclosures of PHI during the process of identifying a patient and locating the record.
{478}

IX.C. TRAINING

IX.C.1 The HIE must have policies that identify minimum training requirements for educating authorized users about the policies and procedures for accessing PHI through the HIE.
{479}

IX.D. TERMINATION OF ACCESS AND OTHER SANCTIONS

IX.D.1 The HIE must have policies that outline the access termination process for authorized users and the process to impose sanctions for violators.
{480}

CRITERIA X: AUDIT

Narrative Summary indicating how the evidence reflects compliance with Standard X.

All PHI accessed will be recorded in an audit log.

X.A. MAINTENANCE OF DISCLOSURE LOGS

X.A.1 The HIE must have policies for the maintenance of disclosure logs by the HIE and/or participating organizations for the systems at which authorized users access PHI, including:
- The identity of the patient whose PHI was accessed;
- The identity of the authorized user accessing the PHI;
- The identity of the trading partner with which such authorized user is affiliated;
- The type of PHI or record accessed (e.g., pharmacy data, laboratory data, etc.);
- The date and time of access; and
- The source of the PHI (i.e., the identity of the trading partner from whose records the accessed PHI was derived).

{481}

X.A.2 The HIE must have controls that secure disclosure logs from alteration regardless of access privilege and that log any attempted alterations.
{482}

X.A.3 The HIE must have policies that require disclosure logs to be maintained for at least six years from the date when the information was accessed.
{483}

X.B. PATIENT ACCESS TO DISCLOSURE INFORMATION

X.B.1 The HIE must have policies that provide patients, upon request, with access to information from the HIE and/or participating organizations about disclosures of their health information.
{488}

X.B.2 The HIE must have policies that require patients be informed of the availability of such information on any patient portals maintained by the HIE.
{489}