MEMORANDUM

SUBJECT **Comments on EHNAC HIE Accreditation Program (HIEAP) Draft Criteria Version 1.0**

DATE **August 25, 2010**

TO **Lee Barrett**
Executive Director
ENACH

FROM **Dan Rode**
dan.rode@ahima.org
(202) 659-9440

CC **Harry Rhodes**
AHIMA Practice Leadership

Below are comments from the American Health Information Management Associations(AHIMA) Health Information Exchange (HIE) Practice Council on Electronic Healthcare Network Accreditation Commission (EHNAC) Health Information Exchange Accreditation Program (HIEAP) Draft Criteria Version 1.0. The Practice Council is a specialty advisory group within AHIMA's governance structure and the comments are those of the Council and not of AHIMA as a whole in as much as the Council took this review process on as its own project. If EHNAC would like involvement of AHIMA we would be pleased to consider it.

In addition to having a Practice Council involved in health information exchange, we have a number of AHIMA members and staff involved in various aspects of HIE at both the federal and state level in governance activities as well as technical and standards activities. AHIMA also administered the Office of the National Coordinator's State Level HIE project for the last four years **(~~www.slhie.org~~).** AHIMA has also address HIE as part of its on-going campaign to see the adoption and implementation of standard electronic health records (EHRs) and healthcare industry interoperability). More information can be found on our website at **www.ahima.org.**

Mr. Harry Rhodes is AHIMA's director of practice resources and lead liaison to the HIE Practice Council. Specific questions on the information below can be directed to me at the above phone or e-mail address, or to Mr. Rhodes at (312) 233-1119 or **harry.rhodes@ahima.org.**

The Practice Council welcomed the opportunity to review the HIEAP criteria and look forward to future opportunities for input. Of note, the Practice Council did not comment on every guideline listed in the draft criteria. Rather, those items that members felt were significant are noted below.

The draft criteria set is sectioned into ten (10) major sections 1) Privacy and confidentiality, 2) Technical Performance, 3) Business Practices, 4) Resources, 5) Security, 6) Consent, 7) Authorization, 8) Authentication, 9) Access and 10), Audit which are appropriate to the type of accreditation being discussed and flow appropriately. There are of course, items that cross into more than one major section and for purposes of the accreditation will need to be restated in section.

The proposed normal site review which is required is 1 day. If all documentation is not presented prior to site visit, if the time required to review documentation requires longer than 1 day additional fees for additional site visit may be required.

The criteria have mandatory requirements that must be addressed in the self assessment, and any mandatory criteria that are not fully completed will cause the candidate to fail the site review.

Although the mandatory criteria have a checkmark to indicate that they are mandatory, the wording on all but one item (II.A. 2.) of the 100 or more items in the criteria states that "candidate must".

SubGroup General observations:

- Will each guideline require evidence of performance (similar to accreditation bodies such as The Joint Commission) and levels of compliance?
- Does the term "provider" utilized throughout the criteria mean strictly a physician or does it encompass other staff acting on the physician's behalf, e.g. nurse, physician assistant, or office staff?
- General concern that some of the technology and functionality listed in the criteria is well beyond the industry's current capabilities.

Section 1		
I.A 3	**..use PHI about individuals only as is necessary for the processing of appropriate electronic transmissions as authorized by the trading partner.**	**Not all activity in the HIE is electronic transmissions. It would be more appropriate to say ...for uses that the trading partner has authorized.**
I.A 4	**<u>Candidate must</u> refrain from selling or otherwise using PHI in such a way as to violate privacy or confidentiality.**	**Many HIEs are looking at clinical data repositories as a potential source of revenue either to aggregate data for research purposes (de-identified), or other use – It would be more appropriate to be only as agreed upon with the trading partner.**
I.A 6	**Must use effective …..malicious software.**	**Define effective – Even the best protections sometimes fail. Is it enough to have reputable, correctly installed and updated with real time detection and alerts? Instead of requiring an effective control; would suggest that the candidate must demonstrate compliance with an existing industry standard i.e. NIST.**
Note I.A 5 through I.A 12		**These may be more appropriately placed in the security section**
Section 2		
II.A 1.	**…receive and submit 100% of all eligible transactions electronically from and to all…accept or generate transactions**	**Not necessarily 100% but …100% of eligible transactions as agreed upon by trading partner(s).**

	electronically.	
II.A. 3	**…make available real time transactions**	**Not all transactions need to be real time, or does having any real time transaction meet criteria? Provide real time transactions as agreed upon in trading partner service level agreements. Define the use of the word limitations.**
II.A 4	**….all applicable federal and state requirements and regulations.**	**What happens when there are conflicts in this area? State and federal requirements and regulations are not always in harmony. There must be guidance for appropriate process when requirements and regulations are contrary between states (harmonization policy).**
II.B.	**All conformance criteria in section II.B should be covered by the trading partner contractual agreements.**	**This is actually a service level agreement and should be negotiable between the trading partners.**
II.C	**All conformance criteria in section II.C should comply with national standards. Timeliness is also contractual type of agreement.**	**This is actually a service level agreement and should be negotiable between the trading partners.**
II.G.2	**…implementation plan …at least sequence and timetable for implementation within mandatory timeframes.**	**This is not a generic item.. the sequence and timeline is heavily dependent on the actual rules and guidelines.**
II.G. 3	**…current analysis…**	**…A lawyer working on this full time would be hard pressed to keep up … Plan is not generic it would be specific to the laws.**
II.H	**Editing capabilities for administrative transactions**	**Define administrative transactions (?ADT?, Document registration, Query?)**
II.J	**99.5% availability on communication exchange components**	**This should actually be addressed in service level agreements only.**
II.K	**Seven years minimum retention to be in compliance with HIPAA. Recommend developing II.K.2 that addresses audit trail functionality rather than combining retention and audit trails in one item.**	**HIE are new to the world – I don't think any of them could actually provide seven years at this point.. This should be broken into two (2) separate items. 1)the mandatory item should be clear and accurate audit trail permitting … 2)the second item should be "A plan to maintain this audit trail for" … Is seven years the appropriate length for retention of the audit trail?**
II.M . 1. and II.M. 5.		**These appear redundant. Recommend to delete II.M.5 as information is contained in II.M.1.**
Note on II.M.		**In general many of the items discussed within II.M appear to be more relevant**

		to security, which is detailed in criteria V.
III.A. 3		**Verbiage regarding "endanger compliance with EHNAC" is confusing and could be worded better.**
III.B. 2	**…interconnecting to other HIEs…**	**Does not specify format (e.g. HL7) for electronic communication between HIEs. In addition, should this be worded "Or to the NHIN" as many HIEs will connect with the NHIN for electronic communication.**
III.D. 1	**..demonstrate formal relationships…**	**The term "formal relationships" alludes to a contractual agreement or memorandum of understanding. Criteria should clarify if a more formal business relationship is necessary or revise verbiage.**
IV.C. 1	**…sufficient qualified personnel…**	**What is the criteria for "sufficient" qualified personnel? And how will this correlate with employee versus contract employee.**
IV.C. 2	**…effective, relevant job training….**	**Define "effective" job training? Suggest revising or eliminating this verbiage.**
V.B. 5 and V.B. 6		**Essentially V.B. 5 and V.B.6 are redundant, suggest combining and revising verbiage for one criteria.**
IV.C.3 and V.B.12		**Redundant – add management to IV.C.3**
V.C. 7.	**…P&P including a log..receipt and removal of hardware and electronic media that contain Electronic PHI….movement within the facility.**	**Will an exception for encrypted PHI be included? Laptops, for example, may go in and out on a daily basis. Would this be a part of the log, even if the laptop is encrypted? In addition, shouldn't a log of paper PHI movement be kept also?**
V.C. 11	**…retrievable exact copy…before movement of equipment where PHI is stored.**	**Is the criteria specific to <u>any</u> movement or just those that include movement to another physically separated site, removal or destruction? Suggest revising verbiage as it currently appears very stringent and implies any movement (even within the same cabinet/rack).**
VI.A 1 Review at full PC Meeting	**<u>The HIE must</u> have policies that allow patients the option of granting or affirmatively denying consent for providers to access their protected health information (PHI) via the HIE.**	**There are several concerns with the criteria, as it is written. 1)Technology At this point in time the granularity of consent is generally opt in / opt out in a universal set for the HIE. Some HIEs can utilize consent by dates**

	Of note: The Subgroup has several concerns with the criteria listed here, please review and discuss carefully. **"We have an opt-out model so a patient's information is included unless they request to opt-out. We are including our status of HIEM in our NPP. The only document we plan to store would be their request to opt-out.** **So, from our perspective we don't want to obtain consent for every patient. The use of the HIE is minimal if we have no patient data in it until consent is obtained."-TWaugh** **Although this may not be technologically possible at this time, the patient should always have the right to request granular level types of restriction requests (i.e., by provider). When the facility reviews the restriction request, they may have to inform the patient that they do not have the capability for that level of restriction and there for will have to either globally opt-in or globally opt-out the patient. But the policy should exist to allow for consideration of those types of patient requests, more of which can be enforced as we advance the functionalities of the HIEs.**	**of service, some can utilize consent based on the provider organization but not necessarily on the specific individual provider.(STorzewski)** **2)functionality, Generally the patient consents (either actively/opt in or passively/opt out) to have records placed in the HIE.** **3)burden of proof, HIEs do not usually have face to face interaction with the patients and are not in position to gather consent paperwork** **4workability I believe that adding additional steps to the consent and or access processes will have negative effects on both participation and use** **For example, what about the case where the patient consents to have their information included in the HIE – once it is there a separate consent is not required for the provider to access it via the HIE. If a provider is querying the HIE for patient information, it is assumed that there is a physician/patient established relationship or they are in the process of establishing the relationship.** **Is the burden on the HIE to ensure that a consent has been obtained?** **Member Comment: I believe the burden of proof would lie with the facility that opts the patient in. They must maintain the consent. Others accessing the information would assume consent has been obtained. As far as specific providers accessing the data, having a physician/patient relationship is assumed and they are ethically bound to only accessing data that they have right to access. No different than EHRs where a physician really could access any patient record, but they are expected to only access those**

		that they are treating or consulting on. Audit trails can be used to monitor. **Current system technology and functionality does not seem to be in sync with this criteria (e.g. At present if using an authorization model to access the records - the current technology could force an alert or pop up when the physician queries the HIE. The pop-up would be asking the provider to verify that patient authorization has been obtained (and can be provided upon request of the HIE / in case of an audit of access.)**
VI.E.		**How will the HIE indicate that "sensitive information" is withheld without in fact indicating that sensitive information exists?**
VI.H.1	**If the provider deems that the information contained within the HIE is material to emergency treatment.**	**How can a provider deem the information material to emergency treatment before he/she looks at it?**
VI.K	**<u>The HIE must</u> have policies that do not require consent by the HIE, its participants, or a government agency to access de-identified data for purposes reviewed and approved by the HIE.**	**Recommend consent purposes follow HIPAA requirements for de-identified data and trading partners are also included.**
VI.P.1	**<u>The HIE must</u> have policies that allow affiliated providers to be consolidated on the consent form if: (i) it lists each participant with sufficient specificity to provide reasonable notice to the patient as to which provider may access the patient's information pursuant to such consent form and (ii) it provides the patient with the option to select which of the providers listed on the consent form may access the patient's information. Any participant accessing information based on a consent form covering multiple providers must be identified on such consent form at the time the patient grants consent.**	**(i) Recommend reviewing this criteria. How will each participant be listed on the consent form, in a large HIE there could numerous providers and as new providers join, how will they be added?** **(ii) Recommend reviewing the verbiage on this criteria as current functionalities may not accommodate opt out at the provider level.** **In general, the criteria does not address where and how are the various documented consents stored? And who obtain the consent signature as HIE's do not "see" patients?**

VII.B	**HIE Administrators with access to PHI for purposes related to public health reporting; …**	**Recommend reviewing these criteria as HIE administrators may need other access to PHI for other uses, such as merging duplicate patients in the MPI. HIE Administrator access to PHI should follow current HIPAA treatment, payment and operations guidelines.**
VII.B. 1.	**The HIE must have policies that restrict the category of authorization of access to the HIE based on authorized user's employment responsibilities and affiliation with the patient.**	**Recommend that the verbiage be clarified to include two (2) separate items.** **1)user employment responsibilities** **2) affiliation with the patient.** **Access and authorization guidelines should further be restated to comply with HIPAA access and authorization requirements.**
VIII.B. 1.	**The HIE must have policies that assign a unique name and/or number for every authorized user.**	**Recommend revising the term "name" and replace it with "access key."**
VIII.C. 1.	**The HIE must have policies that require the HIE to validate the accuracy of the authentication of the authorized user.**	**Recommend that this verbiage be restated to be "In accordance with HIPAA security guidelines the HIE must…."**
VIII.D. 1.	**The HIE must have policies that authorized users provide authentication at every attempt to access the HIE.**	**Recommend clarifying this verbiage. In its current form, it implies that even if a HIE staff remains logged in when accessing a new patient the staff would have to log on again. Recommend revising the term "attempt" to "initiated session."**
IX.A. 1.	**The HIE must have policies that require each authorized user to be assigned a unique user name and password.** **Authorized users shall be authenticated;** **Passwords shall meet the password strength requirements outlined in NIST SP 800-63;** **Group or temporary user names shall be prohibited;** **Authorized users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords; and** **Authorized users shall be prohibited from sharing their user names and/or passwords**	**Recommend reviewing this section as some items are duplicates of previously stated sections.** **If the section remains recommend revising "unique user name" to "access key" as previously noted.** **Recommend guidelines provide additional information on NIST SP 800-63 contents.** **Question the stringency of "totally prohibiting" the reuse of passwords. Agree to verbiage that accommodates a limitation on reusing passwords. For example, users cannot reuse passwords for six (6) password changes.**

	with others and from using the user names and/or passwords of others.	**Recommend revising verbiage to this section that "prohibits reusing passwords for XX number of password changes?" and state "password changes are limited to XX changes within a specified time period." May also include verbiage that requires each password to be a certain length, utilize a combination of alpha and numeric characters, and at contain least one symbol (e.g. Gar@1abc).** **Also recommend that the accrediting bodies develop a standard password module that is required of all HIEs in order to standardize this requirement.**
X.A. 2.	**Audit logs cannot be altered.**	**Recommend adding verbiage "In accordance with HIPAA regulations…"**