

# **INFORMAL PUBLIC COMMENTS**

**RECEIVED ON**

**COMAR 10.25.18, HEALTH INFORMATION EXCHANGES:  
PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION**

On March 14, 2013, MHCC released a second informal draft regulation for COMAR 10.25.18. In response to the invitation for public comments, written comments were received from a total of 17 organizations and individuals. All written comments are included within.



ACCOUNTABLE CARE ORGANIZATIONS  
OF MARYLAND

April 25, 2013

Christine Karayinopulos  
Center for Health Information Technology  
Maryland Health Care Commission  
4160 Patterson Avenue  
Baltimore, MD 21215

RE: Informal Comments on Second Draft - HIE Regulations

Dear Ms. Karayinopulos:

Attached, please find a recommended change to the draft HIE regulations. I am submitting this comment on behalf of three Medicare Shared Savings Program Accountable Care Organizations (ACOs): Western Maryland ACO, Eastern Shore ACO, and Lower Shore ACO. As you may know, the ability to coordinate care as an ACO is heavily dependent on the secure sharing of protected health information. It is equally important that ACOs function as a united system, much like other health care organizations.

As noted in the template, our physicians recommend that the regulations be amended to exclude ACOs, as defined by federal law, from these regulations. An analogous exemption was provided for hospitals and their practitioners that are accessing HIE data through a hospital source. It is our understanding that the Commission is trying not to include daily clinical work in the new regulation. To that end, failure to exempt ACOs and their communications with participating professionals in a manner consistent with the hospital/provider exemption will create a significant barrier to an ACO's exchange of data with its participating professionals and staff for clinical and care coordination purposes.

I appreciate the opportunity to comment on the regulations. Please feel free to contact me if you have follow-up questions regarding ACOs and the attached comment.

Sincerely,

Craig R. Behm  
Executive Director

**Maryland Health Care Commission**  
***Draft Informal Health Information Exchange Regulations***  
**Comment Form**

Individual/Organization Name: <i>Accountable Care Organization of Western Maryland, the Eastern Shore, and the Lower Shore</i> Date: <i>April 25, 2013</i>		
Section	Concern	Recommendation
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection
.01 A Scope		
.01 B Scope		
.01 C Scope	.01(C ) does not include an exclusion for Accountable Care Organizations (ACOs) and their communication with participating professionals, although an exclusion is provided for hospitals for analogous communication with thier professionals.	Add an exclusion to this section for ACOs as defined in 42 CFR Part 425 and/or the Affordable Care Act, Section 1899 that is consistent with the exclusion provided for hospitals and their professionals so that an ACO does not have to be licensed as an HIE if it is using data for the purposes of clinical integration among providers.
.01 D Scope		
.02 B Definitions		
.03 A Consumer Rts		
.03 B Consumer Rts		
.03 C Consumer Rts		
.03 D Consumer Rts		
.03 E Consumer Rts		
.03 F Consumer Rts		
.03 G Consumer Rts		
.04 A Sensitive PHI		
.05 A Access		
.05 B Access		
.05 C Access		
.05 D Access		
.05 E Access		



Maryland Health Care Commission  
4160 Patterson Ave.  
Baltimore, MD 21215

Re: Comments to Proposed draft Regulations for Health Information Exchange

Dear Sirs and Madams:

Thank you for the opportunity to submit informal comments to the second draft of regulations for Health Information in Maryland. The new draft has made some overall improvements in the form and drafting, making the text more clear, concise and easy to use. We noticed some policy changes. We feel some of the changes improve the regulations, while others do not, as noted below.

1. Protected Health Information (PHI), Health Information, and Information derived from PHI:

The revised regulations include, in their scope, “ a person who uses or discloses information derived or obtained from, or based on protected health information obtained or released through an HIE”. Specifically, disclosure of this derivative information is prohibited where the data relates to a person who has opted out. We support this change, and suggest the addition of “health information,” as well.

If a person has not opted out, it appears that the regulations regarding authorization, authentication, and audit apply only to “PHI”. PHI and Health Information are defined in .02. It should be noted that PHI, as defined in HIPAA, excludes health information created or received by an employer, school or university, while “Health Information” does not. In addition, “health information” appears to include data without patient identifiers. It appears that the section on “secondary use” includes PHI, information derived from PHI, and “Health Information”. For persons not opted out, we would suggest that all of the privacy protections and access requirements for primary uses of data should apply to “health information”, in addition to PHI.

2. Secondary Use

The regulation lists a variety of secondary uses to be permitted in the interim before regulations are adopted governing secondary use. More specificity is needed regarding who may conduct these activities and how data may be accessed and handled. It would be preferable to postpone secondary use of PHI, Health information, and information derived from PHI until regulations are in place. If strictly limited to aggregated and anonymized data, we would agree to this in theory, provided that, at the very least, these entities are directly involved in the health care delivery system, and can establish a legitimate

AMERICAN CIVIL  
LIBERTIES UNION OF  
MARYLAND

MAIN OFFICE  
& MAILING ADDRESS  
3600 CLIPPER MILL ROAD  
SUITE 350  
BALTIMORE, MD 21211  
T/410-889-8555  
or 240-274-5295  
F/410-366-7838

FIELD OFFICE  
6930 CARROLL AVENUE  
TAKOMA PARK, MD 20912  
T/301-270-2258

WWW.ACLU-MD.ORG

OFFICERS AND DIRECTORS  
ALLI HARPER  
PRESIDENT

SUSAN GOERING  
EXECUTIVE DIRECTOR

C. CHRISTOPHER BROWN  
GENERAL COUNSEL

public interest in the activity conducted with the information. Marketing, as defined in the HIPPA (45 CFR Sec. 164.501) should be explicitly excluded.

### 3. Opt Out

There is no complete opt-out option in the regulations. A person has no right to opt out of the uploading of her information to a database accessible to the HIE. Even though the information is not allowed to be disclosed for treatment purposes, it may be disclosed electronically for various other purposes listed in .03 A. (2). Unfortunately, we live in a world fraught with hackers and identity theft and spying and tracking and profiling made possible by the computer age. For those, or other reasons, some people will prefer not to participate at all in HIE. Studies have shown that avoidance of medical care or withholding of information during medical encounters may result from a lack of trust in the privacy of medical records. There is general agreement that consumer trust is critical for HIE to succeed. Therefore, there should be no upload of records of those who opt out.

The regulations should be clarified to make clear that, while, at the very least, a consumer must be allowed to opt out, that it is also permissible to operate an HIE on an “Opt-In” basis.

### 4. Point to Point Transmission

The rationale for exempting point to point transmissions from the regulations is not clear to us. We cannot understand why the same considerations of privacy and security would not apply to these events. The requirements in the regulations are meant to insure that only those who are authorized may gain access to information, for an authorized purpose, that the sender and receiver may be confident in one another’s identity, and that the information is secure. The regulations are not there to impede or burden but to facilitate the exchange of information needed to provide medical care. We do not see why point-to point transmissions, if they are done through the HIE, should not be governed by the regulations.

### 5. Patient Consent Options

We note that assent to query has been removed, so that patient choice is completely lacking for those not opted out. The Policy Board has expressed its desire to encourage HIE’s to implement patient choice mechanisms as soon as practicable. We had requested a report on technical solutions for granular patient choice from the State-designated HIE, which was not delivered, due to changing circumstances. Until a clear and unbiased understanding of the technical feasibility of implementation emerges, patient choice should not be completely left out of the regulations. Technology will continue to evolve and adapt, provided it is incentivized to do so. Assent to query was a compromise

interim policy pending more information on emerging technical solutions. The regulations should reflect this policy in some meaningful way or else there will be little incentive to implement patient choice.

## 6. Payor HIE's

We are concerned that the Policy Board has not had the opportunity to inform itself and discuss the implications of explicitly authorizing payors to operate HIE's. We recognize that, absent specific authorization, payors are not prohibited from operating HIE's. However, before making a decision to affirmatively authorize payor HIE's, we believe the Policy Board should be given a chance to examine the issues and determine whether there are concerns that should be addressed with granting payors access to information that they do not already have by virtue of claims processing, or other lawful functions of the health insurance business.

## 7. Entity Holding Information

We do not believe a special exemption is warranted for information accessed within the same organization where the records are held. If the HIE is utilized for these transactions, the same considerations of role-based access should be applied, in order to insure that those viewing records are authorized, are who they claim to be, and that the records are accessed for a purpose they are authorized to carry out.

## 8. Rights of Minors

Under the current draft, it appears that records regarding minors are treated the same as those of adults. We believe there are concerns specific to minors' records that require careful consideration. Choices made by parents and others will have lasting consequences after a consumer is no longer a minor child. The interplay between the statute allowing minors to consent to certain medical treatments and the HIE should be thought through. The regulations in New York provide that minors between the ages of 10 and 18 are excluded from the HIE. We suggest that in the interim, Maryland should follow the New York precedent.

## 9. Specific proposed edits

.01 Scope and Purpose: include in scope, " and, where specified, 'Health Information' and ' information derived or obtained from, or based on protected health information obtained or released through an HIE'."

.01 C. (2): delete

## .02 Definitions

B (11): delete “outside the entity holding such information”

(16) delete “is created or received by...clearinghouse”. ( limiting the definition of Health Information in this manner may have unintended consequences and does not appear to be necessary)

(17) delete: “A payor may act as....regulations.”

(25) delete “request” and substitute “election” and delete “that the patient has elected”.

(34) (d) delete “or permitted by law, including those set forth in Health-General Article, Sec. 4-305(b), Annotated Code of Maryland.” This is a very broad category of types of disclosures with numerous possible unintended consequences. Section 4-305(b) lists a variety of circumstances when a physician may disclose a patient’s health information without the patient’s consent, including when there is a lawsuit, for medical research, and many other things not within the purview of primary uses. The Policy Board drew the line between “required by law” (primary use) and “permitted by law”(a secondary use) after careful deliberation.

## .03 Rights of Health Care Consumer

C. (1) (a) Insert after “participating organization”: “ that maintains health information accessible through the HIE”

C. (3) (a) 30 days seems a long time to simply inform a consumer of how to request a correction. Substitute “10 days.”

C.(4) Add: “health information, or information derived from health information” to what a consumer may request a report of.

D. add: health information and information derived from PHI.

E. (2) add: “health information”

E. (3) delete “permitted” and substitute “required.” Disclosure of “deidentified” information is permitted by law, which would render this section meaningless.

G. This section requires more specificity. For example, merely posting a sign in the office should not suffice. Add: “ no later than the first medical encounter following the enrollment of the provider in an HIE, patients must be given written and oral notice, including...”

## .06 Auditing

C. The standards in the prior draft for audit have been removed. We believe there should be some requirement of standards for audits. We suggest that the deleted standards be replaced. “The audit shall be: Objective; Proactive; Systematic, and In accordance with current generally accepted industry practices.”

E. (3) The new version is less transparent to the consumer. We suggest requiring either posting of the yearly audit, or a requirement that it must be available to consumers upon request.

.07 Remedial Action by HIE

C. (4) We believe the consumer should be notified whenever an investigation results in a reasonable belief that a breach or violation has occurred, as provided in the prior draft.

.09 Registration and Enforcement: A consumer who is entitled to notice under section .07 should be given some rights in this section to notice, submission of information, and entitlement to be informed of the final disposition of an enforcement action involving the consumer’s information.

We hope that these comments assist in developing regulations for a robust Health Information exchange that is secure and private, and that will improve the delivery of health care for the people of the State of Maryland.

Respectfully Submitted,

J. Sarah Posner, Esq.  
For Sara N. Love, Esq., Public Policy Director  
ACLU of Maryland

Brian England  
British American Auto Care

Over the years of attending meetings I have spoken out in support of using the latest technology to communicate to the consumer when their PHI has been accessed in a HIE. Notification technology has advanced a lot even over the past year and is now in common use and it should be incorporated into the regulations.

Any communication system should notify the consumer that their PHI has been accessed and by whom, this can be done by "Notify" "Text" "E-mail" etc..... this would be up to the consumer. (If local governments can do this type of notification so should a HIE).

If the system is going to be a success then there must be consumer confidence in the system, electronic notifications will be a great step towards the public acceptance.

Here is my change to .03 Rights of a Health Care Consumer.....  
Section C. part (4)

Replace current part (4) with

"An HIE shall provide a health care consumer a written report on request or a electronic notification that details any disclosure through the HIE of the PHI."



.03 A Consumer Rts	Implies that we must allow the consumer to see what is in our HIE	We may want to put in some boundaries as to what it means to show this information to the individuals. For example, we may want to say that Dr. Notes are excluded. Hard to say as it will not be popular with civil liberties advocates but it is a concern in that we've been told that Providers will not be candid if they think their notes will be read by patients.
	Commits us to an education plan. It isn't clear how much information is to be provided (iii) and (iv).	
.03 C Consumer Rts	<p>It is unclear what context this falls. Would the consumer be inquiring about a specific piece of PHI (e.g. a lab test) or in general? If specific, how is it referenced? "Where did you get this lab data?" vs "Where did the lab data you provided to my Provider come from?"</p> <p>Concerned about how the inquiry is made and the implications on how to find the data listed. Also concerned if this is at a literal data element "My record shows a A1C of xx. Where did that come from?" I don't think that we have ready access to that level of accounting. Equally concerning would be a general fishing expedition "Tell me where all of my data is coming from."</p> <p>"Type of PHI" is ambiguous. Is at the level of "Clinical Record vs Lab Data vs ADT"? What is expected?</p> <p>(3) This appears to be at a field level - e.g. "I think my x lab value is wrong". What if we got it from multiple sources? (c) says we have to notify any participating organizations who have accessed the data that has been corrected. How will we know it has been corrected? That will occur in the source system and may never be sent. A record locator is still valid but unless someone asks for the data it won't be sent. Even if sent, we won't know it has been corrected unless the source organization tell us. How far back do we have to go in the notification? We won't likely know when it was incorrect.</p> <p>2 (b) - 7 days may be too short. For what time period are we obligated to tell - past 30 days, 6 months, 7 years?</p> <p>Does "providing data to the HIE" include the locator record or the literal response to an inquiry? If it is an aggregator model, does it only pertain to information accessed?</p> <p>(4) commits us to keep a log of who saw what for 7 years.</p> <p>(d)(i) The PDF reports should count as the "two/year".</p>	<p>The hie will make a good faith effort to supply the information stored within its system or available through record locators to the authorized consumer about that consumer for a reasonable time period not to exceed 6 months. This information may exclude direct coordination of care provider to provider communications. In the event that a consumer believes that an error exists in their records, the hie will make available the list of participating organizations which have provided data and/or record locators to the hie for the consumer. The hie will also make best efforts to publish the consumer and the nature of the dispute to participating organizations which have provided health information for the consumer in question. In the event that the hie aggregates or otherwise stores health information, the hie will make best efforts to correct its data stores upon receipt of certification from a qualified provider that the information was incorrect and the corrected data has been supplied. this provider must be part of an active participating organization. This satisfies the hie's role in helping the consumer resolve data related issues. HIE shall facilitate the resolution by informing the health care consumer how to correct these errors... records that are inappropriately attributed.</p>
.03 D Consumer Rts	(2) (c) This should only apply to what is confirmed as a breach.	Add the following at the beginning of (2) c "Once a breach is confirmed"...
.03 E Consumer Rts	<p>Since this is an opt out model, do we only need to track the periods for which the member opted out (1)? All other periods are implicitly opted-in.</p> <p>(2) There has to be reasonable time to process the consumers request to opt out. As written, this is "instantaneous". (F) (4) (a) sets this at 5 business days.</p> <p>(3) Strongly object to not being able to use a patient's data under secondary use if they have opted out. Agree that it can't be used as PHI but should be allowable as de-identified data per HIPAA regulations. We do this constantly with Groups and with PCMH.</p>	
.03 F Consumer Rts	<p>(3) Should the word "appropriate" be replaced by "reasonable"? This could be a heavy burden and very difficult to verify.</p> <p>(5)(b)(v) We're expected to send a Text?? It is an "or" so it is one method but strange...</p> <p>(6) will be challenging to administer</p>	
.03 G Consumer Rts	<p>(1) How does this work in a network of networks? Does the participating organization simply tell the consumer about the HIE to which they are connected? By calling us an HIE, this could impact our PCMH consents (why do I want to give CF the access?).</p> <p>(2) Is this implying that the participating organization is obligated to notify consumers of a breach that occurred at the HIE? It seems like this is redundant and puts a burden on the Provider. The HIE should have to notify of its breaches just as the participating org has to notify of its breaches.</p>	Strike 1b

.04 A Sensitive PHI	Restricts "Sensitive Data" to Point-to-Point. Under the carve out for hospitals, this allows them to still communicate this but we would have to pull any data that falls under this out of the MHR. We don't have the ability to do this as it is co-mingled in the notes. Our consent covers both types of data. Will that give us the right? By having the language under .04 A (1) does that make it out of compliance even though we have consent? (2) makes it seem so. Also, under (2), is that consent a one-time or per instance? (3) Why isn't this handled just like any other inappropriate access under HIPAA?	Strike 2b restriction to point-to-point. Our MHR doesn't comply with that. We are obtaining consent to share this data.	
.05 A Access	A - How does this work if the participating org isn't in MD? Does that matter? Will this require us to change all of our Provider contracts and the other PCMH/TCCI contracts? How long do we have once this goes into effect? (2) Isn't stating that we need a BA redundant as this is PHI? What's the intent of calling it out again?		
.05 B Access	B (1) How can the HIE validate or enforce this? We know that it is an authorized user but we would have no way to know what they intend to do with the data. (2) This doesn't seem to read correctly. The HIE shall only disclose data if the data may be incorporated into the participating org's EHR? Why is this tied to what the HIE can/can't do? It should just be another point in the document where they describe participating orgs. -	Strike B(2)	
.05 C Access	C (1) allows "population-based" use but the earlier opt-out allows for a consumer to opt-out of the population making it invalid. - (Ji) suggested changes in .03 e (3) would cover this		
.05 D Access			
.05 E Access	(1) by having this at each user vs a role with user-specific audit data, we severely limit SSO and complicate the required coordination. SSO should allow for assertions. (1) (a) (i) is already required under HIPAA (1) (a) (ii) This is open ended. What level of "assistance" is required and what liability does that shift to the HIE? If it is limited to education on roles and enabling it technically, it is OK. (1) (b) Should state that we have a reasonable timeframe for doing so. What is the difference between (1) (a) (ii) and (2)? (4) (a) should not preclude SSO (4) (c) or adequately protected from unauthorized access (5) LOVE 5 but it is inconsistent with earlier text. As written, (5) supports SSO assertions. It is silent on the need for the assertion to send user-level audit information. Don't know if we want to suggest adding that or not.	E (4). Where a user logs in directly to the HIE, <the rest of the language is Ok - just need to ensure that this is a callout for direct login and doesn't apply to the SSO mentioned under (5)> What about when it comes through a handoff and two level authentication has already occurred?	
.05 F Access	(2) How is the participating org supposed to ensure this? Is written attestation from the 3rd party sufficient? (2) (b) or attest that the login data is adequately protected from improper access - To require it to be encrypted will likely knock out several 3rd parties that need to participate. (2) (c) asking 3rd parties to have two factor auth will also knock out too many parties (3) Does notification of (b) or (c) constitute a breach at the HIE? I wouldn't think so. I think the breach is at the participating org. What is the HIE's obligation once notified? Wouldn't want this to trigger the breach process for the HIE.		
.05 G Access	(2) <b>ABSOLUTELY NOT!!!!</b> Doing this will be an administrative nightmare and compromising one part org compromises all. HIE's should have to implement SSO using SAML 1.x or higher with defined roles that are common across all HIE's passing agreed upon audit data that, while meaningless in a systematic way at the recipient clearly captures the unique individual for whom the access is granted. The asserting org has the accountability to authenticate properly and assign the appropriate role and audit data. (5) add (c) or for those individuals for whom access is no longer appropriate	Strike (2) and add the comment for 5c: <b>" or for those individuals for whom access is no longer appropriate" DELETE</b> *the possibility of duplicate user names and passwords. Need to ensure common protocol for authentication and authorization.	

.06 A Audit	<p>(1) Can't develop "each specific circumstance". Most of these are unknown. The HIE can develop a methodology and monitoring approach that aims to do this but the HIE can't warrant that it is complete or foolproof.</p> <p>(2) very vague. What constitutes a "random" audit? Looking at one random record? Statistically valid sample? What is "more frequently than monthly"? Every 29.5 days? "Notified by a person about an unusual finding"???? Shouldn't it say "in cases where the HIE has reason to believe that inappropriate access may have/or is occurring"?</p> <p>(5) (b) within two business days of what? Being notified? Determining that finding was unusual? Same for (c)</p> <p>(d) (ii) Does state and federal requirements spell out the retention of logs?</p>	<p>(1) Develop and implement a protocol that defines circumstances that constitutes an unusual finding to be identified within an audit of the user authentication logs (2) At least monthly, conduct a random audit of the user authentication logs to identify any unusual finding; (b) If the unusual finding involves between ten and 50 patients, within five business days of validation of an unusual finding; (c) If the unusual finding involves more than 50 patients, within three business days upon validation of the unusual finding</p>	
.06 B Audit			
.06 C Audit	<p>This seems redundant to the required, periodic HIPAA Risk Assessments that covered entities are expected to conduct. The only difference here is that there are a few things asked here that are more specific than HIPAA like the encrypted storage of credentials and the requirement to accept SSO. This also specifies a time period - annual whereas HIPAA only says periodic. This also grants the Commission the right to require an external assessor.</p>		
.06 D Audit	<p>(2) "within the timeframe specified by the Commission". Needs to have some boundaries such as within 45 days of the written request of the commission. Keep in mind that if the commission requires a 3rd party, that would require us, under Federal Procurement Guidelines, to RFP that engagement and enter into a contract BEFORE the assessment.</p>	<p>In (2), specify 45 days vs "within the time...."</p>	
.06 E Audit			
.06 F Audit	<p>(2) This seems to only apply to "non-HIPAA" aspects. Not clear on what "non-HIPAA" means and sweeps in.</p> <p>(3) The HIE will only provide data within the logs pertinent to the requesting Participating Org.</p>	<p>(3) The HIE will only provide data within the logs pertinent to the requesting Participating Org.</p>	
.07 A Redial Actions			
.07 B Redial Actions	<p>(1) No later than the next business day is unreasonable.</p> <p>(4) Can't constrain this saying that you have to finish within 14 business days (why 14 and not 15....). I can see that the HIE must respond within 15 days and, if the investigation is not completed, must explain why it isn't completed and the time table for completing the investigation. Not clear who this would be reported to...the Commission?</p>	<p>(1) The HIE shall begin the investigation as soon as practicable but no later than three business days after learning of the allegations giving rise to a potential breach or non-HIPAA violation; (4) Upon the completion of an investigation, which shall not exceed 30 business days, an HIE shall</p>	
.07 C Redial Actions	<p>(2) Providing this to each person within 10 business days may not be reasonable if the breach is large (it shouldn't be since these are the people suspected of the breach and not the people impacted). Where the breach is suspected of a person at a Participating Org, the HIE should notify that org as well.</p> <p>(2) (b) Not sure what remedial action we expect the people committing the breach to do other than stop. Seems like we are communicating under this section information to the wrong parties. We should notify the person we believe is causing the breach of their obligation under the Part Agreement but I wouldn't think we would give them specifics.</p> <p>(2) (d) How is the HIE supposed to know who, at the participating org, should perform the actions? That should be their responsibility, not the HIE's.</p>	<p>1) The HIE shall begin the investigation as soon as practicable but no later than the next business day after learning of the allegations giving rise to a potential breach or non-HIPAA violation</p>	
.07 D Redial Actions			
.07 E Redial Actions			
.08 A Breach			

.08 B Breach			
.08 C Breach			
.08 D Breach			
.09 A Reg/Enforcement			
.09 B Reg/Enforcement	(2) references a financial viability audit pointing back to .07 but there didn't seem to be anything in that section dealing with financial viability of the HIE.		
.09 C Reg/Enforcement			
.09 D Reg/Enforcement			
.09 E Reg/Enforcement			
.09 F Reg/Enforcement			
General Comments	Need information on how the Commission is formed, its membership, how people become members, terms, etc.		
General Comments			



Chesapeake Regional Information System for our Patients  
7160 Columbia Gateway Drive, Suite 230, Columbia, MD 21046

T: 877.952.7477 W: [www.crisphealth.org](http://www.crisphealth.org) E: [info@crisphealth.org](mailto:info@crisphealth.org)

To: David Sharp

From: David Horrocks, CRISP

Date: 3/22/13

RE: Draft HIE Regulations

---

CRISP would like to thank the MHCC for the opportunity to comment on the latest pre-publication draft of the HIE regulations provided for informal comment. In general CRISP believes that this draft of the regulations is significantly improved in terms of appropriateness and usability as a result of MHCC's ongoing outreach to members of the health care community in Maryland and the responsiveness of the MHCC to the input it received.

**.02 B. (3)**, definition of "Authorized Purpose", requires that, for disclosures for daily operations and maintenance, the staff of the HIE or the staff of a contractor have signed a confidentiality agreement. This will be difficult to implement as to the staff of a contractor, which may change over time and which, in any event, is not under the direct supervision of the HIE. The contractor will be a HIPAA business associate and under confidentiality obligations as to members of its work force. We think that the interests of the public will be sufficiently protected if the HIE requires (in addition to the HIPAA Business Associate Agreement for any contractor which maintains or has access to the data in the HIE technology) a contractual undertaking that the contractor will limit access to members of its work force to those with a "need to know" and who are under a confidentiality restriction, which may be a work force policy and procedure bringing on the work force member.

**.02 B. (17)**, definition of "HIE", refers to an exclusion for organizations "not under common ownership". While Maryland hospitals may have further comments, CRISP believes that the phrase should be "common ownership *or control*", to account for the various organizations structures in some Maryland health systems.

**.03 A. (2) (a)** describes a right to opt-out and situations in which information may still be disclosed. In general, we believe directed communications between physicians, which are the functional equivalent of today's faxed documents or secure email, should be permissible even when a patient has opted out. At the same time, we can imagine certain direct messages which

are automated from which it might be best to give consumers the right to opt-out. Further consideration might be necessary.

**.03 C. (1)** specifies information which must be supplied to health care consumers about records “available through the HIE”. We read this to apply to information which is query-able and not to directed messages which might have traversed the HIE without persisting. An HIE may not have records of the latter. We believe that the regulations should be more specific on this point.

**.03 C. (4) (b) (ii)–(iv)** defines information that must be provided to an individual from an HIE on request. CRISP has two concerns. First, identifying the name of the organization with which the authorized user is affiliated on a disclosure-by-disclosure basis in accordance with C. (4) (b) could be done but would be difficult and would require going outside of CRISP’s current records structure, imposing a time and cost burden that might be the same for most HIEs. Second, the draft regulations do not provide a procedure for furnishing a summary of recurring disclosures to the same entity for the same purpose. Such a provision, CRISP believes, would serve the purpose of this section but pose a lesser burden on HIEs.

**.03 E. (3)** prohibits disclosure of de-identified data “derived from a patient’s PHI” who has opted out. While recognizing that de-identification and then use of individual records may not be in the public’s interest in all circumstances, we believe that when such records are merely part of a “count” that their inclusion is important. For instance, CRISP is providing hospitals a “count” of statewide readmissions for the prior month. Excluding opted out patients from such a count could make the reporting of such trends inaccurate, with no corresponding benefit to patient privacy. We think adding an exception at the end of this sentence would be appropriate, such as “... or such information is limited to including counting the individual in a numerical field”.

**.03 F. (2)** does not recognize a phone call to the HIE as a means of opting out. While a definitive record of an opt-out may be easier to maintain when in writing or online, it is CRISP’s experience that many opt-outs do come by phone. While CRISP offers no position, MHCC may want to consider ease of opting out in this section.

**.05 G. (1)** requires a system administrator to “note the individual’s assigned username and password” however it is highly unusual and violates best practices for a system administrator to know a user’s password.

**Maryland Health Care Commission**  
**Draft Informal Health Information Exchange Regulations**  
**Comment Form**

Individual/Organization Name: <u>    IDX-SASD Monique Harold - Coventry    </u>		Date: <u>    3/29/2013    </u>
Section	Concern	Recommendation
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection
.01 A Scope		
.01 B Scope		
.01 C Scope	2) definition of point to point interfaces	Does this include EDI (HIPAA Txns)/claims/enrollment interfaces? Does it include EDI transactions? What about web services to display PHI to the member it applies to, i.e. a member calls up their own lab results or a child's results?
.01 D Scope		
.02 B Definitions	17) Definition of "HIE" is not clear. In this context Coventry is an HIE? or does Coventry have to operate as a separate legal entity to be an HIE? 8c) The opt-out language is unclear; what are the consumers opting out of? Just the electronic exchange of information? Or opting out of sharing information altogether? 33) Does point to point transmission include information sent in support of a claim or authorization?	17) It is not clear if HIE implies the exchange or Coventry as a company. If HIE means Coventry, then all subsequent sections need to be analyzed. The definition needs clarification. The document implies that everything that applies to HIEs applies to Coventry. We need confirmation that everything is applicable. We understand for this review that Coventry is a participating organization, and not the HIE. 8c) Remove the option fo exchanging information in a paper-based system. This language is confusing. The patient should be opting out of information exchange, whether electronic or not. 33) Once the information is attached to a claim or authorization it becomes viewable by any authorized user. If there is a requirement to restrict just this information then this will impact the claims system.
.03 A Consumer Rts	2c) Who does the notifying?	2c) If the participating system does the notification then Coventry's portals/HIX vendor relationships are affected.
.03 B Consumer Rts		
.03 C Consumer Rts		
.03 D Consumer Rts	1) If Coventry is acting as the HIE, there is an impact to auditing across	1) Clarify which information is tracked by the HIE, and which is tracked by each participating organization.
.03 E Consumer Rts		
.03 F Consumer Rts	4) Timing of the 5 business days may not be enough to communicate the changes from the HIE, to HPS/enrollment portals, through IDX and to all downstream systems.	4) Recommend 10 business days
.03 G Consumer Rts		
.04 A Sensitive PHI	The indicator if member approval is needed for exchange PHI is probably needed from health insurance exchanges.	Are the HIX vendors sending this information? This requirement may be difficult to comply with if this must be done this year. What is the effective date for this legislation?
.05 A Access		
.05 B Access		
.05 C Access		
.05 D Access		
.05 E Access		
.05 F Access		
.05 G Access		
.06 A Audit	This statement implies the requirement to have an enterprise level audit/review of authentication logs. Is this the case?	It appears we need a complete audit since a member/claim might flow through many different systems. We have audits in individual systems but not across systems. If this is required across systems there will be modifications to several systems, esp. to include the new opt-out information
.06 B Audit		
.06 C Audit		
.06 D Audit		
.06 E Audit		
.06 F Audit		

.07 A Redial Actions		
.07 B Redial Actions		
.07 C Redial Actions		
.07 D Redial Actions		
.07 E Redial Actions		
.08 A Breach		
.08 B Breach		
.08 C Breach		
.08 D Breach		
.09 A Reg/Enforcement		
.09 B Reg/Enforcement		
.09 C Reg/Enforcement		
.09 D Reg/Enforcement		
.09 E Reg/Enforcement		
.09 F Reg/Enforcement		
General Comments	Timing of the legislation	When is the compliance date for this legislation? If it coincides with the Health Insurance Exchange implementation, it may be difficult to meet the timelines
General Comments	Opt-out process	Define specifically what the patient is opting out of. Point to point transmission does not appear to include EDI transactions, or information we provide to downstream vendors. This will negatively impact us if we have to start using paper because the member opted out.
General Comments		
General Comments		
General Comments		

**Maryland Health Care Commission**  
**Draft Informal Health Information Exchange Regulations**  
**Comment Form**

Individual/Organization Name: <i>Steve Daviss MD, FUSE Health Strategies LLC</i>		Date: <i>4/29/2013</i>
Section	Concern	Recommendation
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection
.01 A Scope	.01.A(3): "To improve access to clinical records by treating clinicians" ... My comment is that this is a critical issue to address, and patients with mental health or substance use disorders (MHSUD) should also enjoy improved access to their clinical records. The majority of patients treated for these conditions want their primary care providers to be aware of their MHSUD and the medications and treatment they are receiving. A recent Hopkins study showed that hospitals that restrict access to patients' psychiatric records such that their nonpsychiatric physicians cannot access them have a higher readmission rate than those hospitals who permit access to their records. The claims costs of patients with chronic medical conditions with comorbid MHSUD is nearly double the costs of those without comorbid MHSUD. There should be no additional barriers to accessing patients' mental health and Part 2 records beyond that of obtaining required consent. Preventing HIE access to these records, and instead requiring point-to-point access only, adds a barrier to access that will continue the discriminatory treatment that these patients have historically received. We implore you to consider permitting HIEs to use the necessary technical adjustments (e.g., Rhode Island) that permit MHSUD patients to enjoy the same benefits of HIE that all other patients receive.	There should be no additional barriers to accessing patients' mental health and Part 2 records beyond that of obtaining required consent. Preventing HIE access to these records, and instead requiring point-to-point access only, adds a barrier to access that will continue the discriminatory treatment that these patients have historically received. We implore you to consider permitting HIEs to use the necessary technical adjustments (e.g., Rhode Island) that permit MHSUD patients to enjoy the same benefits of HIE that all other patients receive.
.01 B Scope		
.01 C Scope		
.01 D Scope		
.02 B Definitions	.02.B(32)(b) "Person in interest" means ... (b) An INDIVIDUAL authorized to consent to health care... : We believe that this should state "person" rather than "individual." The reason is that the definition of a "person" includes a trust, partnership, LLC, the State, etc. There are many situations when the State or a legal firm or another entity is authorized to consent. The current definition would not include these entities under the definition of "person in interest." Person in interest should include "persons" not "individuals."  .02.B(32)(e)(ii) Here, this should be changed from "An individual authorized to consent..." to "A person authorized to consent..." for the same reasons stated above.  .02.B(34)(e) There appear to be incompatible statements here. "...including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose..." By their very nature, clinical guidelines are intended to be based on "generalizable knowledge." It is not clear why this phrase is included here, as quality improvements activities are	.02.B(32)(b) Change (b) as follows: "A PERSON authorized to consent to health care..."  .02.B(32)(e)(ii) Change (e)(b) as follows: "A PERSON authorized to consent..."  .02.B(34)(e) We suggest STRIKING the rest of the sentence after "...clinical guidelines."
.03 A Consumer Rts		
.03 B Consumer Rts	.03.B(1)(b)(iii) Insert capitalized text as follows: "The specific details concerning who may access, use, or disclose a patient's health information AND SENSITIVE HEALTH INFORMATION and for what purpose;" Reason: the education plan should address patients' rights regarding sensitive health information and this needs to be spelled out due to the extra precautions. Similar language should be inserted in .03.B(1)(b)(v), as well.	.03.B(1)(b)(iii) Insert capitalized text as follows: "The specific details concerning who may access, use, or disclose a patient's health information AND SENSITIVE HEALTH INFORMATION and for what purpose;"  .03.B(1)(b)(v) Similar language should be inserted in .03.B(1)(b)(v), as well.
.03 C Consumer Rts		
.03 D Consumer Rts		
.03 E Consumer Rts		
.03 F Consumer Rts		
.03 G Consumer Rts		

.04 A Sensitive PHI	<p>This entire section, while probably well-meaning, prevents patients with mental health or substance use disorders (MHSUD) from enjoying the full benefits of an HIE by permitting only point-to-point transmission of MHSUD information, including Part 2 records and mental health records as defined in Health-General Article 4-305 to 309 (mental health records are different than the "personal notes" also referred to in 4-307). Such a limitation adds an additional barrier to communication of important sensitive health information among a patient's providers, especially when that patient may have authorized such disclosures. Such a limitation is contrary to public health policy and continues the discriminatory treatment that these patients have historically received.</p> <p>A recent Hopkins study showed that hospitals that restrict access to patients' psychiatric records such that their nonpsychiatric physicians cannot access them have a higher readmission rate than those hospitals who permit access to their records. The claims costs of patients with chronic medical conditions with comorbid MHSUD is nearly double the costs of those without comorbid MHSUD. There should be no additional barriers to accessing patients' mental health and Part 2 records beyond that of obtaining required consent.</p> <p>We implore you to consider permitting HIEs to use the necessary technical adjustments (e.g., Rhode Island) that permit MHSUD patients to enjoy the same benefits of HIE that all other patients receive, without requiring a default to point-to-point transmission for sensitive health information. SAMHSA has addressed the myth that 42 CFR Part 2 regulations prevent the transmission of these records via HIE. The links below explain these issues in more detail.</p> <p><a href="http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf">http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf</a>  <a href="http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf">http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf</a></p> <p>To quote SAMHSA's FAQ: "This consent requirement is often perceived as a barrier to the electronic exchange of health information. However, as explained in other FAQs, it is possible to electronically</p>	<p>We implore you to consider permitting HIEs to use the necessary technical adjustments (e.g., Rhode Island) that permit MHSUD patients to enjoy the same benefits of HIE that all other patients receive, without requiring a default to point-to-point transmission for sensitive health information. SAMHSA has addressed the myth that 42 CFR Part 2 regulations prevent the transmission of these records via HIE. The links below explain these issues in more detail.</p> <p><a href="http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf">http://www.samhsa.gov/healthprivacy/docs/ehr-faqs.pdf</a>  <a href="http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf">http://www.samhsa.gov/about/laws/SAMHSA_42CFRPART2FAQII_Revised.pdf</a></p>
.05 A Access		
.05 B Access	<p>.05.B(2)  Suggest inserting the capitalized text to address redisclosure of records that are incorporated into the patient's medical record: "...may be incorporated into the patient's medical record kept by such participating organization AND MUST FOLLOW ALL STATE AND FEDERAL LAWS REGARDING</p>	<p>.05.B(2)  Change as follows: "...may be incorporated into the patient's medical record kept by such participating organization AND MUST FOLLOW ALL STATE AND FEDERAL LAWS REGARDING REDISCLOSURE OF RECORDS."</p>
.05 C Access		
.05 D Access		
.05 E Access		
.05 F Access		
.05 G Access		
.06 A Audit		
.06 B Audit		
.06 C Audit		
.06 D Audit		
.06 E Audit	<p>.06.E.  This paragraph provides a threshold of improper use, access, or disclosure ("more than ten patients") at which additional steps must be taken. However, it does not specify how many total patients must be included in the audit. Thus, if an audit only examines 30 records, it would take 11 patients with improper use before these additional steps are taken. MHCC must decide what is an acceptable percentage of audited patients with improper use before specifying this number. We doubt that 33% is an acceptable threshold, thus this section should either specify the minimum number of audited patients (not just records) OR should specify the percentage of patients with improper use, access, or disclosure, that would trigger these additional steps.</p> <p>.06.E(3)  We recommend deleting the first five words of this paragraph ("If requested by the Commission"). In the interest of transparency for Maryland health care consumers, the summaries of ALL audits should be routinely made publicly available on the HIE websites, and should not only be triggered by MHCC request. Additionally, in the last sentence of this paragraph, the word "may" should be changed to "shall": "...and the Commission SHALL also post the report on its website." Having all the HIE audit</p>	<p>.06.E. This section should either specify the minimum number of audited patients (not just records) OR should specify the percentage of patients with improper use, access, or disclosure, that would trigger these additional steps.</p> <p>.06.E(3)  We recommend deleting the first five words of this paragraph ("If requested by the Commission"). Additionally, in the last sentence of this paragraph, the word "may" should be changed to "shall": "...and the Commission SHALL also post the report on its website." Having all the HIE audit summaries in one place is a patient-centered approach to transparency.</p>
.06 F Audit	<p>.06.F(3)  This paragraph indicates that participating providers that have the HIE conduct its audit as per .06.F(1) shall quarterly review the HIE logs in a particular manner, but initial sending of the logs is only triggered by a request by the participating provider. Requiring that the provider request the logs is an unnecessary step where something could be forgotten. Because .06.F(1) can already trigger an HIE audit, this section should be changed to state that the participating provider shall review the logs within 10 days of the HIE sending them. An additional requirement should be that the HIE send the logs</p>	<p>.06.F(3)  This section should be changed to state that the participating provider shall review the logs within 10 days of the HIE sending them. An additional requirement should be that the HIE send the logs quarterly.</p>

.07 A Redial Actions		
.07 B Redial Actions	.07.B. This paragraph should be edited to delete the last part, "or a violation of Part 2 has occurred." The reason for this edit is that "non-HIPAA violation" already includes Part 2 violations, so by including this phrase, it would call into question the applicability of this section to other non-HIPAA violations, such as violations of Health-General 4-307. Removing this confusing reference should reduce this potential for ambiguity.	.07.B. This paragraph should be edited to delete the last part, "or a violation of Part 2 has occurred."
.07 C Redial Actions		
.07 D Redial Actions		
.07 E Redial Actions		
.08 A Breach		
.08 B Breach		
.08 C Breach	.08.C(1) Remove "individual" and replace with "person" in two instances: "If the entity providing the notification under this Regulation has knowledge that another PERSON is acting as the health care consumer for the patient, the entity shall provide the notification to that PERSON instead of the patient." Reason: the definition of a "person" includes a trust, partnership, LLC, the State, etc. There are situations when the State or a legal firm or another entity is authorized to consent as a person in interest, so this paragraph should use the more inclusive term, "person."  .08.C(4) This paragraph uses a "reasonable time frame" of notification of 60 days from discovery. Because of the concern of a breach resulting in identity theft (as stated in .08.C(5)(b)), which, if it happened, could cause much damage in such a long time frame, we suggest using a much shorter time frame here, such as three days or five days.  .08.C(5)(f) This section states that a notification shall include various bits of information and contact resources, but it does not mention including contact information for MHCC. We suggest adding the following: "(iii) The Maryland Health Care Commission."	.08.C(1) Remove "individual" and replace with "person" in two instances: "If the entity providing the notification under this Regulation has knowledge that another PERSON is acting as the health care consumer for the patient, the entity shall provide the notification to that PERSON instead of the patient."  .08.C(4) We suggest using a much shorter time frame here, such as three days or five days.  .08.C(5)(f) We suggest adding the following: "(iii) The Maryland Health Care Commission."
.08 D Breach		
.09 A Reg/Enforcement		
.09 B Reg/Enforcement		
.09 C Reg/Enforcement	.09.C(2) This paragraph addresses issuance of a notice of proposed enforcement action to a person in violation. There needs to be clear notice to the person, not just placing the notice on the MHCC website. We suggest revising this paragraph as follows: "After needed investigation, the Commission staff may issue a notice of proposed action VIA CERTIFIED MAIL that includes the following:"	.09.C(2) We suggest revising this paragraph as follows: "After needed investigation, the Commission staff may issue a notice of proposed action VIA CERTIFIED MAIL that includes the following:"
.09 D Reg/Enforcement		
.09 E Reg/Enforcement		
.09 F Reg/Enforcement		
General Comments	The benefits of HIE should apply to all participating consumers, including those with mental health and substance use disorders. The barriers to achieving this have been worked out in other HIEs, so Maryland should not lag behind in addressing the needs of consumers with complex needs... If anything, they need the benefits of HIE even more so.	
General Comments		

March 20, 2013

Christine Karayinopulos,  
Center for Health Information Technology,  
Maryland Health Care Commission,  
4160 Patterson Avenue, Baltimore, MD 21215

Dear Ms. Karayinopulos:

This communication is regarding the MHCC Seeks Informal Public Comment on Draft HIE Regulations; second draft of the health information exchange regulations.

My comments regarding the draft regulations follow:

1. On page 6 and 7, under (15)  
Consider inserting “ (b) (vi) a pharmacy (this is inconsideration of the pending HB1310 change in “Definition of Health Care Provider” –see bill on following page), and multiple other Maryland Law identifying pharmacists as providers. Patients seek and receive care at their pharmacy to include, dispensing prescription drugs, assistance in identifying and selection of over the counter medications, exempt laboratory tests, point of care testing monitoring, counseling on medications, blood pressure screenings, vaccinations, medication reconciliation, medication regimen review, and other services.

2. On page 12, under (2) The right to opt out of a health information exchange.  
(a) A health care consumer has the right to opt out  
Consider inserting (a) (v) “Results of prescription medications dispensed/filled sent to the provider who ordered the prescriptions or another provider as designated by the ordering provider

Thank you for your consideration.

Regards,

Jennifer Thomas, PharmD

HB 1310

Department of Legislative Services

Maryland General Assembly

2013 Session

FISCAL AND POLICY NOTE

House Bill 1310

(Delegate Dumais, et al.)

Judiciary

Health Care Malpractice Claims - Definition of "Health Care Provider"

This bill alters the definition of "health care provider" for purposes of a health care malpractice claim. The bill must be construed to apply only prospectively and may not be applied or interpreted to have any effect on, or application to, any cause of action arising before the bill's October 1, 2013 effective date.

Fiscal Summary

State Effect: The bill does not directly affect governmental operations or finances.

Local Effect: The bill does not directly affect governmental operations or finances.

Small Business Effect: Minimal.

Analysis

Bill Summary/Current Law: Under current law, for purposes of a health care malpractice claim, "health care provider" means a hospital, a related institution, a medical day care center, a hospice care program, an assisted living program, a freestanding ambulatory care facility, a physician, an osteopath, an optometrist, a chiropractor, a registered or licensed practical nurse, a dentist, a podiatrist, a psychologist, a licensed certified social worker-clinical, and a physical therapist, licensed or authorized to provide one or more health care services in Maryland.

A "related institution" is an organized institution, environment, or home that maintains conditions or facilities and equipment to provide domiciliary, personal, or nursing care for two or more unrelated individuals, admitted or retained by the institution for

HB 1310/ Page 2

overnight care, who are dependent on the administrator, operator, or proprietor for nursing care or the subsistence of daily living in a safe, sanitary, and healthful environment. A "freestanding ambulatory care facility" is defined as an ambulatory surgical facility, a freestanding endoscopy facility, a freestanding facility utilizing major medical equipment, a kidney dialysis center, and a freestanding birthing center.

The bill repeals the current definition of "health care provider" and specifies, instead, that a "health care provider" is (1) a health care facility, center, or program licensed under Title 19, Subtitle 3 of the Health-General Article (which includes a hospital or a related institution) or (2) a person licensed, certified, or registered under the Health Occupations Article, which includes a multitude of therapists, technologists, counselors, practitioners, assistants, and professionals within the scope of the health care malpractice subtitle (such as an acupuncturist, a pharmacist, a physical or occupational therapist, an athletic trainer, a physician assistant, a respiratory care practitioner, a radiation oncology technologist, and a professional counselor or therapist).

The bill further specifies that "health care provider" includes an employee, volunteer, or agent delivering or assisting in the delivery of health care services of any or the aforementioned entities or persons.

Current law also specifies that “health care provider” does not include any nursing institution conducted by and for those who rely upon treatment by spiritual means through prayer alone in accordance with the tenets and practices of a recognized church or religious denomination. This provision is unchanged by the bill.

**Maryland Health Care Commission**  
**Draft Informal Health Information Exchange Regulations**  
**Comment Form**

Individual/Organization Name: <i>The Johns Hopkins Health System Corporation</i>			Date: <i>April 26, 2013</i>
Section	Concern	Recommendation	
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection	
.01 A Scope			
.01 B Scope			
.01 C Scope			
.01 D Scope			
.02 B Definitions	In Subsection (34), the definition of "Primary use of HIE data" or "primary use" in Subpart (d) is limited to "other disclosure[s] required or permitted by law..." Under this definition, certain <b>uses</b> (as opposed to disclosures) of the data maintained by the HIE that would otherwise be permitted by law, such as for research with appropriate IRB approval or health oversight activities, would not be considered a primary use under these regulations. Since the use of such information for research purposes or health oversight purposes is also not included in the categories of uses permitted as a "secondary use," use of the HIE data for these critical and important activities would not be permitted by these regulations. By unnecessarily restricting a participating organization's ability to use data from the HIE for these types of activities, the regulations may unintentionally prevent the advancement of medical research and the ability of a participating organization to use a valuable resource of data for the oversight of the health care system. Since a participating organization is otherwise permitted to use health data for these purposes under HIPAA and State privacy laws, the source of the data should be irrelevant and participating organizations should not be prohibited from utilizing an HIE to simplify and streamline access to this data.	We propose that Subpart (d) be revised as follows: "(d) Other <b>use[s]</b> or disclosure[s] required or permitted by law, including those set forth in Health -General Article, §4-305(b), Annotated Code of Maryland..." This change would permit the use of HIE data for those activities otherwise permitted by law, such as research and health oversight activities.	
.02 B Definitions	In Subsection (34), the definition of "Primary use of HIE data" or "primary use" in Subpart (e) includes as a primary use of the HIE, "health care operations as defined by HIPAA, for conducting quality assessment and improvement activities..." It is unclear whether the permitted use and disclosure under this subpart is conducting quality assessment and improvement activities only, or whether the permitted uses and disclosures under this subpart include all health care operations activities permitted by HIPAA. To the extent the intent of this language is to limit uses to quality assessment and improvement activities only, by limiting the uses and disclosures of data accessed through the HIE to only these activities, these regulations would prevent a participating organization from utilizing a valuable tool to conduct other worthwhile and necessary activities that are otherwise permitted by privacy and security laws, such as HIPAA and the Annotated Code of Maryland. HIEs can be highly valuable tools for participating organizations to access data necessary for performing medical reviews or other auditing activities, contributing to the effectiveness of an internal compliance program, and other business planning and development activities. HIEs employ technology that permit participating organizations to manipulate even their own data for these purposes and being able to utilize the HIE for these purposes could save a participating organization significant amounts of time and resources in gathering and organizing data. Since these types of activities are permitted by other privacy and security laws, it seems illogical for the participating organization to be prohibited from utilizing HIE data for these purposes. As stated in our comments above, the source of the data should be irrelevant, and participating organizations should be able to use the data retained by the HIE for these otherwise permissible purposes.	We propose that the definition include all permitted uses and disclosures for health care operations as defined in HIPAA, so we would suggest revising Subpart (e) as follows: "health care operations as defined by HIPAA, <b>including without limitation</b> , outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities." This would clarify that quality assessment and improvement activities are just examples of the types of uses and disclosures that would be considered a primary use under these regulations and that any uses or disclosures that qualify as a health care operation under HIPAA would be included as a primary use.	

.03 A Consumer Rts	<p>Subsection (b) provides a carve-out for sensitive health information which would require providers to avoid using or disclosing this data for all purposes if a health care consumer has opted out of the HIE. One of the disclosures permitted under these regulations generally, even if a health care consumer opts out of the HIE, is the right to disclose information when required by Federal or State law. If Federal or State law requires the disclosure of information, even sensitive health information, the disclosure should be permitted. A carve-out of this permitted disclosure for sensitive health information as set forth in Subsection (b) creates a complication where a disclosure may be required by a Federal or State law, but these regulations would prohibit such disclosure, since it contains sensitive health information. For example, participating organizations are currently required to perform certain of its mandatory State reporting through the State's designated HIE. To the extent that information contains sensitive health information, participating organizations would be put in a position where the State is requiring the participating organization to do its mandatory reporting through the HIE, but these regulations prohibit that activity. Furthermore, it may not be feasible for the participating organization to remove all the information that meets the definition of sensitive health information prior to making these required reports. As noted in this same Subsection (b), sensitive health information already receives additional protections under the regulations in .04, so providing this carve-out is unnecessary and places avoidable complications on disclosures required by Federal or State law.</p>	<p>We propose deleting Subsection (b) entirely, so there is no carve-out for sensitive health information and any disclosure required by Federal or State law would be permitted.</p>
.03 B Consumer Rts		
.03 C Consumer Rts		
.03 D Consumer Rts		
.03 E Consumer Rts		
.03 F Consumer Rts		
.03 G Consumer Rts		
.04 A Sensitive PHI		
.05 A Access		
.05 B Access		
.05 C Access		
.05 D Access		
.05 E Access		
.05 F Access	<p>Subsection (1) states that "a participating organization shall designate a system administrator who is capable of carrying out the requirements set forth in Regulation .06D(2)..." Regulation .06D(2) references an HIE's responsibility to conduct additional unscheduled audits.</p>	<p>We believe the cross-reference to .06D(2) is an error and should be to Regulation .05G. Regulation .05G is the provision that sets forth those measures that the participating organization's system administrator is responsible for carrying out. Therefore, Subsection (1) should be revised as follows: "a participating organization shall designate a system administrator who is capable of carrying out the requirements set forth in Regulation .05G..."</p>
.05 G Access		
.06 A Audit		
.06 B Audit		
.06 C Audit		
.06 D Audit		
.06 E Audit		
.06 F Audit		

.07 A Redial Actions		
.07 B Redial Actions		
.07 C Redial Actions		
.07 D Redial Actions		
.07 E Redial Actions		
.08 A Breach		
.08 B Breach		
.08 C Breach		
.08 D Breach	<p>Subsection (1) requires each participating organization to report all violations of federal or State privacy or security laws to the appropriate federal or State authorities. This requirement is very vague and unclear. It is unclear what is meant by "appropriate federal and State authorities," and requiring participating organizations to notify federal and State authorities to which they do not otherwise have a legal obligation to report to is unduly burdensome.</p>	<p>We propose that this requirement be revised as follows: "Each participating organization and each HIE shall report all violations of federal or State privacy or security law to <b>those federal or State authorities to which reporting such violation is required by applicable law</b>, whether or not such law is specifically set forth in the regulations."</p>
.09 A Reg/Enforcement		
.09 B Reg/Enforcement		
.09 C Reg/Enforcement		
.09 D Reg/Enforcement		
.09 E Reg/Enforcement		
.09 F Reg/Enforcement		
General Comments		

**Maryland Health Care Commission**  
**Draft Informal Health Information Exchange Regulations**  
**Comment Form**

Individual/Organization Name: <b>KAISER PERMANENTE</b>		Date: <b>4/29/13</b>
Section	Concern	Recommendation
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection
.02 B Definitions	"Non-HIPAA violation" should be refined to be clear that it is specific to privacy violations. As is, it is so broad that it will not be clear what is supposed to be included.	We suggest that this term mean "a use, access, or disclosure that is not a HIPAA violation, but is not permitted by Part 2 or the Maryland Confidentiality of Medical Records Act."
.02 B Definitions	The term "person in interest" includes an attorney appointed in writing by an individual listed in this definition. An attorney is not a healthcare decision maker for a patient, unless they are otherwise designated as a surrogate, in which case the definition already covers that role. Attorneys otherwise have no special authority to obtain medical information as opposed to anyone else that the patient may authorize under a release of information. Including them here would include them as a "health care consumer" throughout this regulation and would allow them to get patient health information that they otherwise may not be entitled to other than through a HIPAA authorization. The reason for this access seems primarily to assist in litigation or as a means of receiving communications from a health care provider regarding their client's medical information, which is an inappropriate use of an HIE, and would discourage participation by health care providers.	Delete (f) from the definition of "person in interest" so it no longer includes "an attorney appointed in writing by an individual listed in this definition."
.02 B Definitions	It is not clear who is responsible for creating and maintaining the master patient index, defined in paragraph 22.	Clarify responsibility for creating and maintaining the master patient index.
.03 A Consumer Rts	Under paragraph A (2) (a), a health care consumer has the right to opt out of a health information exchange at any time and refuse access to the patient's protected health information through an HIE, with certain exceptions. One exception is when a disclosure is limited to "Federal or State law requirements." This should be clarified. Does this mean when necessary to comply with Federal or State law requirements, such as reporting obligations (this may be duplicative of the exception for reporting to public health authorities), or is this meant to cover all disclosures that are permitted by federal or state law, which would be very broad and would not allow a health care consumer to opt out so long as a disclosure was permitted by State and federal law.	Clarify what is meant by "Federal or State law requirements."
.03 B Consumer Rts	Paragraph E prohibits an HIE from disclosing a patient's protected health information if the health care consumer has opted out, "except as otherwise permitted under applicable law." This also should be clarified, as it can be read to allow the HIE to disclose protected health information so long as that disclosure is permitted by existing privacy laws. That would render an opt out meaningless, as a health care consumer could only opt out of disclosures that were not permitted anyway.	Clarify what is meant by "except as otherwise permitted under applicable law."
.03 A Consumer Rts	Paragraph F (5) requires an HIE to provide each Health Care consumer with the option to receive confirmation of any change in the patient's participation status. If a health care consumer requests such confirmation in writing, the HIE must "provide" the confirmation within 3 business days of the effective date of change. "Provide" is ambiguous in that it could be read to require that the patient receive confirmation within 3 business days, which would not be a reasonable time frame.	We recommend that "provide" be changed to "send."

.03 B Consumer Rts	Paragraph G requires a participating organization to inform each Health Care consumer of the organization's participation in an HIE, including in its Notice of Privacy Practices under HIPAA, and information regarding the right to opt out. A requirement to inform each Health Care consumer, which is defined to include not only patients, but also persons in interest, is overly burdensome. It would include every patient on whom a healthcare provider has a medical record, and those patients' guardians, surrogates, individuals with a medical power of attorney, appointed personal representatives of deceased patients, parents or custodians of minor patients (but not if the parent's authority to consent to health care for the minor has been specifically limited by a court order or a valid separation agreement entered into by the parents of the minor), minor patients if they are able to consent to the care in the medical record, representatives of minors designated by courts (but only in the discretion of every physician who has attended a minor patient), and, as currently defined, attorneys who have been designated by patients. It is not realistic that a health care provider could identify all of these individuals to inform of its participation in an HIE.	Instead, a participating organization should be able to provide information about its participation in an HIE by posting the information on its website and including the information and its Notice of Privacy Practices.
.05 E Access	Paragraph C limits "secondary use" of HIE data to only population based activities. We believe the HIE regulations should deal only with disclosure of health information rather than use. Paragraph C is also confusing as to the distinction between primary versus secondary use, specifically, whether it is intended to prohibit any use other than the initial use for which the information was obtained. The limitation in Paragraph C would be too limiting. For example, the regulation does not appear to permit use of information for quality purposes (non-population-based) if it was obtained for treatment purposes. Sequestering information received through HIE to not allow other uses that are permitted under the law would be burdensome.	Health care providers should be able to incorporate HIE data into its records and retain that information in accordance with the recipient's record retention policies and procedures. The recipient should be allowed to re-use and re-disclose that data in accordance with all applicable law
.07 A Remedial Actions	Paragraph C (3) lists several events that trigger suspension of access. One (b) is the event of a significant non-HIPAA violation by a person, and (c) is the event of a significant violation of State or federal law relevant to privacy or security by a person. It is not clear how these are different, unless suspension is triggered by violation of any law that is not HIPAA, even if the law has nothing to do with privacy or security of medical information, which would be overly broad.	A non-HIPAA violation should be defined as violation of Part 2 or the Maryland Confidentiality of Medical Records Act.
.08 A Breach	Paragraph B (1) (a) requires an HIE to notify the person who notified the HIE of a potential breach or non-HIPAA violation if the HIE concludes there was a breach or non-HIPAA violation. Such notification could be inappropriate if notice requires revealing patient information and the person who notified the HIE is not the patient or the patient's personal representative.	Revise (a) to require notice to "The person who notified the HIE of the potential breach or non-HIPAA violation, if applicable, and to the extent permitted by HIPAA and other Federal and State privacy laws."
.08 B Breach	Paragraph B (1) (c) requires notice to each health care consumer acting on behalf of each patient whose PHI or sensitive health information was inappropriately accessed or disclosed. This notice would not actually include the patient as it is drafted to require notice only to health care consumers acting on behalf of patients.	Instead, "health care consumer" should be replaced with "patient or person in interest."
.08 C Breach	Paragraph B (3) requires substitute notice, which may include publishing the notice on the home page of the entity's website.	The required content of such notice should be clarified, as posting names of patients acknowledging the existence of a medical record could itself violate privacy laws.
.08 D Breach	Paragraph D requires reporting of violations of Federal or State privacy or security law to the appropriate federal or state authorities. These regulations should not create additional requirements for reporting under these laws.	This provision should be clarified to require reporting to appropriate federal or state authorities, "as required by applicable law."



Koss on Care LLC  
2909 Wilton Ave  
Silver Spring, MD 20910

Dear Ms Karayinopulos,

April 29, 2013

Thank you and your MHCC colleagues for the opportunity to comment on the second draft of the initial HIE regulations. The draft rules establish many of the needed components to govern health information exchange throughout the state, however there continue to be some areas that raise confusion about how HIEs will interoperate and how patients will be able to readily access their own information.

Please accept the following comments for further consideration:

Although the scope and purpose section indicates the following goal of the rules “(4) To promote uses of the State-Designated HIE that will assist public health agencies in reaching public health goals.” Other than the definition there is no reference to how this will be advanced. In fact, the rule seems rather silent on the interoperability of HIEs. If we are trying to advance a statewide infrastructure, I believe the requirement to exchange with the state-designated HIE should be included and support the goal of patients being able to access their information wherever it resides throughout the state.

The chosen terminology of “health care consumer”, “patient”, “person”, “person of interest” and “individual” seem rather confusing. It might be preferable to reserve the terms individual(s) and entity(ies) for authorized users or maintainers of HIEs and participating organizations, while leaving the terminology person, patient and consumer, to the people and their proxies, whose PHI is being maintained and shared through HIEs. Section 03.F represents a set of provisions where the terminologies will likely cause confusion because it is unclear that the healthcare consumer and patient are often one and the same.

As a patient/consumer advocate, I want to again strongly recommend that HIEs and participating organizations be required, perhaps over a phased-in time period, to offer consumers a single point of access to their EHR information across the continuum of care. Providers can offer this capability, or HIEs should be authorized to provide the service. Patients should not have to go thumb drive in hand to each provider. HITECH and the efforts of Maryland should not be limited to advancing accessibility solely to the care and payment system while leaving the consumer as the last mile. I would like to see section 03.C.(2) amended to reflect this approach.

Section 03.C.(4) should be amended to enable and preferably require online requests and not just written requests (similar to F.(2)).

Sections 04. A (1) and (2) seem contradictory and could perhaps be made one section in which sensitive health information is either exchange via point-to point or with patient authorization through an HIE.

The section on secondary data use and the definition of secondary data use raise concerns. The definition only gives examples that to many individuals are the greatest cause for concern. A broader less biased set of examples should be included. Subsequently, the list of allowable secondary uses 04.C.(1), absent regulations, are very broad categories of information that could be very much in the eye of the beholder. I know this relies on HIPAA requirements as a backdrop, but some aspects of HIPAA should perhaps be reiterated and some preference for use of limited data set and IRB approval of the need for identifiable data should be included.

06.C and D are a bit unclear when a 3<sup>rd</sup> party will be required. Will this be a requirement each year or will the request only be when there is some indication that there may be problems or unnecessary risks.

Thank you again for the opportunity to comment.

Warmest regards,

A handwritten signature in cursive script that reads "S Koss".

Shannah Koss

President, Koss on Care LLC

Mary Jo Deering, Ph.D  
Office of the National Coordinator for Health Information Technology

Overall, this is a very strong draft. Congratulations to Maryland for developing this draft and getting it out for comment. What follows is a mix of a few small editorial comments and a couple of more substantive questions. I'm not expecting answers of course; I just wanted to share my sense that something wasn't clear to the reader, or where an additional step in a process seems to be needed.

- General comment and, specifically, p. 7 definitions B (17) Health information exchange and p. 33, .09A, on registration to operate an HIE. The name "health information exchange" in fact covers a broad and evolving multitude of models. Have you determined whether any entities based on emerging models might not be covered? Would these regulations apply to a vendor network, like EPIC Care Everywhere, or SureScripts, both of which have customers and cover patients across all states? I'm not trying to single them out, just raise the question of how comprehensive your definition is meant to be and whether there might be any unintended loopholes. My understanding is that Minnesota had to go back and modify early language because key entities that needed to be covered could claim not to fit the initial definition.
- P. 5, Definitions B(7) on Core elements. The word "is" in last line seems ungrammatical.
- General Comment and p. 12 .03.A.(2) and p. 19 .03.G.(1)(b) concerning right to opt out. It's not clear what the mechanism for opting out is. Does the consumer opt out at the individual provider level (and must repeat the action at ever provider) or is does consumer opt out at HIE level? Can consumer opt out of having information shared through a specific participating HIE (I assume they may opt out of having information from specific providers like behavioral/mental health/HIV providers)? Also, do both the participating organizations and the HIE communicate to the consumer about the right to opt out?
- P. 21 .05C, secondary uses. How will you monitor permitted vs. prohibited uses?
- P. 22, .05.E.(5) accepting third party system authentication. How will an entity know that ".. third party system is compliant with these regulation and all applicable federal and State privacy and security regulations"?

- P. 24, .05.G.(5) duties of system administrator to terminate user access under 2 circumstances. Since this is supposed to happen “immediately,” do you want to include an explicit statement about who is responsible for notifying the system administrator about the two categories of users who are supposed to be immediately terminated, and the period of time that should elapse between time suspension or separation from the organization occurs and notification to the system administrator (presume it should also be “immediately”)?

Thank you for the opportunity to comment.

Regards, Mary Jo Deering

Mary Jo Deering, Ph.D.  
Senior Policy Advisor  
Office of the National Coordinator for Health Information Technology  
U.S. Department of Health and Human Services  
355 E Street, SW  
Suite 310  
Washington, DC 20024-3221  
(o) 202-260-1944  
(c) 202-384-6105  
[maryjo.deering@hhs.gov](mailto:maryjo.deering@hhs.gov)



MHA  
6820 Deerpath Road  
Elkridge, Maryland 21075-6234  
Tel: 410-379-6200  
Fax: 410-379-8239

April 29, 2013

Christine Karayinopulos  
Center for Health Information Technology  
Maryland Health Care Commission  
4160 Patterson Avenue  
Baltimore, Maryland 21215

Dear Ms. Karayinopulos:

On behalf of our 66 member organizations, the Maryland Hospital Association (MHA) appreciates the opportunity to provide comments on the draft privacy and security regulations governing the exchange of protected health information through the Health Information Exchange. The public needs to be confident that private details about their health will not be misused, particularly when sensitive conditions or treatments may be involved. Clinicians using an exchange need to be confident that it adds value by enabling them to better follow clinical guidelines, coordinate care with other providers, and obtain relevant information that presents an accurate composite of a patient's health. Inadequate privacy and security controls can lead to public mistrust and reluctance to participate in an exchange. However, overly restrictive controls limit, the usefulness of exchanges, and fail to provide value to users.

We appreciate the thoughtful work and revisions made to the draft regulations since they were last circulated. We believe this draft represents significant improvement:

- Eliminating the requirement that patients opt-in to allow query into the exchange while at the same time preserving the importance of education about the exchange;
- Aligning the definition of "sensitive health information" with information specially protected by applicable law (Section 02.B (39)); and
- Requiring a hospital to have business associate agreements in place with ancillary clinical service providers only when required by HIPAA (Section 01.C(1)(c)).

In a few areas we raise caution, suggest change, or request additional clarity.

**Sensitive Health Information—Section .04.A(1)**

While we agree with the change in the definition of sensitive health information to align with established legal definitions, we caution against the requirement that all sensitive health information exchange occur only via point-to-point transmission. There is a real technical and operational challenge to ensure that no sensitive health information is transmitted through an exchange; for example, a sensitive diagnosis or medication may be included in a patient's past medical history within a clinical summary for an orthopedic admission.

### **Correction of Information—Section .03.C(3)**

MHA appreciates the change in the process to correct health information that a consumer believes to be in error, and believes the regulations are headed in the right direction. The regulations should explicitly state that it is the responsibility of the consumer to contact the provider that originated the data, if the consumer believes there is an inaccuracy.

### **Breach Notification Requirements—Sections .02B(24), .03D, and .08B**

The regulations define the term “non-HIPAA violation” as inappropriate use, access or disclosure that is not a HIPAA violation, but is inconsistent with state or federal law or this chapter. This term describes circumstances more commonly referred to as an actual or potential breach. For the sake of clarity, we recommend replacing all instances of “non-HIPAA violation” with “actual or potential breach.”

Sections .03D and .08 describe processes an exchange must follow in the event of a breach or potential breach. It is unclear whether an Exchange as a business associate can complete this process, nor is it clear how these requirements align with new HIPAA Omnibus breach notification requirements. Moreover, the requirements prescribed by the federal law require separate processes for business associates and covered entities, and potential and actual breaches. MHA recommends that the Maryland regulations reference the federal processes and not establish separate state processes.

### **Secondary Use of Data—Section .05.C**

Clear regulations concerning the appropriate use of secondary data are important. While everyone can think of examples of intrusive and unwanted secondary uses, health information exchanges provide new opportunities, and expectations, that aggregating and analyzing data in new ways is a foundational element to achieving a “learning health system” that improves quality and reduces medical errors, health disparities, and health care costs. MHA looks forward to working with the Maryland Health Care Commission (Commission) staff and the Health Information Exchange policy board to further define regulations concerning secondary use of data.

### **Authentication—Section .05E(4)(b) and (5)**

MHA supports an authentication process that requires more than a single factor to access an exchange. Common practice within hospital systems is to require two-factor authentication to access protected health information. For this reason, we agree that it is appropriate to allow an authorized user of a third-party system access to the exchange when accessed through a trusted third-party system as specified in .05E(5). We would encourage an exchange to accept a wide variety of security measures that may be used by different organizations, including RSA Certification and semantic models.

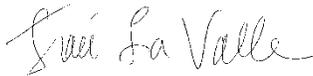
### **Audit Requirements—Section .06**

This section describes a process that an exchange shall initiate when an unusual finding is observed. MHA believes unusual findings should be handled in the same manner as potential breaches.

MHA offers two additional suggestions. In future policy or regulations, we recommend that the Commission consider how protected health information would be handled in the event an exchange ceases to operate. We agree with the Commission that educational materials for the public are an important component of building trust in the exchanges and in helping consumers understand how best to engage in their health care decisions. In developing those education tools, it is important that consumers understand how their information may be used, who may access it, the benefits of their information being available in an exchange, and the technical limitations of exchanges. A realistic expectation of the potential benefits, such as care coordination, should be balanced with the understanding that an exchange may not include all of a person's medical information.

We appreciate the opportunity to comment on these important regulations while in their draft format. If you have any questions, please contact me at 410-540-5087.

Sincerely,

A handwritten signature in cursive script that reads "Traci La Valle".

Traci La Valle  
Vice President, Financial Policy & Advocacy

E. Fremont Magee  
Maryland Institute for Emergency Medical Services Systems

The Maryland Institute for Emergency Medical Services Systems (MIEMSS) provides a web based prehospital medical record system known as eMEDS to Maryland EMS providers.

eMEDS is used to create the patient's prehospital care record as well as to provide public health data to MIEMSS. EMS providers interface with various Maryland hospitals depending on the patient's location and condition as well as the hospitals area of expertise.

I understand from Lisa Myers and John New that David Sharp feels eMEDS in its present form would not be an HIE.

However, there is some concern over a lingering ambiguity regarding whether and how the HIE regulations might affect eMEDS. For example, if eMEDS were an HIE, what would the opt provisions apply to? Could a patient opt out of the patient's medical record?

MIEMSS is considering how this might be addressed in the HIE regulations. I understand that the informal comment period ends today, but I would like to request a few more days for MIEMSS to decide if there is an issue here and to formulate a potential solution that could be part of the regulations. (My current inclination would be to make clear that the HIE regulations do not apply to eMEDS.)

Two other comments I have are:

1. It would seem that an HIE is more a data base or data system or some other infrastructure (not really sure what the means) rather than an "entity". An entity would be the individual, corporation, or government that creates, operates, or maintains the HIE rather than being the HIE. That interpretation is also consistent with the statutory definition of HIE.

Health General § 4-301 defines Health Information Exchange as:  
"...an **infrastructure** that provides organizational and technical capabilities ...".

However, the proposed regulations define Health Information Exchange as"  
"...an **entity** that creates an infrastructure that provides organizational and technical capabilities ..."

Shouldn't the definition of HIE in the regulations be changed so that it is consistent with the statute?

2. Would the State Trauma Registry be an HIE under the proposed regulations?

Cordially,

Monty

E. Fremont Magee  
Assistant Attorney General  
Maryland Institute for Emergency Medical Services Systems  
653 West Pratt Street  
Baltimore, Maryland 21201  
410.706.8531 [fmagee@miemss.org](mailto:fmagee@miemss.org)

**April 29, 2013**

### **Comments on Draft Regulations for Health Information Exchange**

The Mental Health Association of Maryland is a leader in progressive programs resulting in more effective treatment, improved outcomes for individuals, increased research and greater public understanding of the needs of children and adults living with mental illness. MHAMD is proud to represent mental health consumers on the Health Information Exchange (HIE) Policy Board and participate in the process of drafting the HIE policies that resulted in the initial draft regulations in 2012. Many hours of spirited discussion went into crafting related policies, and a balance was struck between consumer protection and allowing HIEs and participating organizations the flexibility to appropriately share information. MHAMD would like to thank the Maryland Health Care Commission for the inclusive and transparent process and for the commitment to considering comments on draft regulations. While thoughtful and comprehensive in some sections, the regulations lack clarity in many others. In order to provide substantial comments, we had to make assumptions (noted where applicable) in certain areas. We encourage the MHCC to use plain language that is more easily understood by consumers and providers and that where possible, does not simply reference another section of regulations or statute as the only definition or explanation. Also, we were dismayed by the removal of some sections of the 2012 draft regulations, which resulted from heavily debated, yet ultimately agreed upon policies and procedures determined necessary by the HIE Policy Board to educate and protect consumers. Unfortunately, MHCC has removed some of these provisions and specificity that was prevalent in the 2012 draft regulations. Our comments in March of 2012 supported that specificity, and the comments outlined on the attached comments sheet will again illustrate the need for strong, specific consumer protection and education requirements. The confusion created by removal of some sections of the regulations and lack of clarity in another, may have an adverse effect on a consumer's decision to opt-out of the HIE.

It is widely recognized that in order for the HIE to function as envisioned and fulfill the promise of advancing care coordination and improving health care outcomes individuals must permit their information to be shared. We continue to believe that the only way to ensure maximum participation in the system is to foster consumer trust in this new health care technology. Consumers must not only be educated on the benefits of participating in the HIE but also must feel confident their information is secure and the safeguarding of it is the top priority of the HIE. MHAMD writes in support of all consumer protection, outreach, and education requirements in the draft regulations as they will create a platform of trust and maintain consumer control over their health care decisions; both of which will likely decrease the number of individuals opting out of the HIE.

Unfortunately, MHCC did not take our recommendation provided in our 2012 comments that the requirements below that empower consumers to make informed decisions about their health

information should be maintained. **We strongly encourage MHCC to reconsider and re-insert them into the final regulations.**

### **.03 Rights of a Health Care Consumer Concerning Information Accessed or Disclosed Through an HIE**

- In the previous draft regulations section 10.25.15.03B(1) provided more detailed requirements of the consumer education plan the HIE must develop and adopt *Providing clear, easy to access information to individuals regarding their rights and responsibilities, and those of the HIE and participating organizations, enables consumers to make informed decisions about their health data.*
- In the previous draft regulations section 10.25.15.03B(1) included a requirement that stakeholders be included in the development in the development of education plans. *This is essential for plans to be effective as envisioned. Stakeholders can play a valuable role in formulating meaningful outreach strategies to engage special populations, including individuals with diagnosed mental illnesses.*

MHAMD appreciates MHCC's commitment to protecting sensitive health information, and we agree that until further regulations are developed, ensuring privacy of this information can best be done by limiting its exchange via point to point transmission. It appears that the scope of the regulation (10.25.18.01C) does not include the point to point transmissions, therefore these transmissions would not flow through or be facilitated by the HIE. However Section 10.25.18.04A(2)(a) requires "consent or authorization consistent with applicable law prior to access, use, or disclosure of sensitive health information to and through and HIE to an authorized recipient." If sensitive health information can only be transferred via point to point, but is permitted to flow through the HIE then the entirety of the regulations must apply to point to point transmission and those participating organizations who employ it. We find no valid reason why the entirety of the regulations should not apply to any information that is transmitted via point to point transmission either through or facilitated by the HIE. In fact, MHAMD argues that the inclusion of education materials regarding how sensitive information can be transmitted is critical to a consumer's ability to make informed decision about their participation in the HIE.

MHAMD's understanding of the proposed regulations is that all mental health records are considered sensitive as the definition of sensitive health records refers to section 403-7 of the Health General Article, which addresses the transmission of all mental health records. If our interpretation is accurate, then while point to point transmission provides an added layer of security for sensitive health information, there appears to be no mechanism for an emergency provider to procure a patient's medical record in its entirety. If the MHCC did not intend that all mental health records be considered sensitive but rather only the psychotherapy notes, which is addressed in Health General 403-7(a)(6) then this must be clarified in the definition of sensitive health records and in section .04 of the regulations, which addresses their transmission. Understanding the difficulty in addressing everyone's concerns and the limits of the current point to point transmission systems, MHAMD looks forward to working with the MHCC and the HIE policy board to develop policies and subsequent regulations that will protect sensitive health information while providing for more accessibility for providers to this critical information. We are confident that CRISP will soon be able to facilitate the accessibility of sensitive health records through the HIE while protecting the privacy of consumers.

As requested we used the attached comment form for the majority of our comments, but it does not allow for feedback denoting support for requirements that are critical for building consumer trust and that must be preserved in their current form. **The following must be maintained in the regulations:**

**.03 Rights of a Health Care Consumer Concerning Information Accessed or Disclosed Through an HIE**

- 10.25.18.03(A) the right of consumers to access information regarding their rights and to refuse access to their health information through the HIE, or opt-out. *This is the only sure way to give consumers control over their health information*
- 10.25.18.03(C) the right of a consumer to access their protected health information through the HIE or if not feasible that the HIE will facilitate a consumer's ability to access this outside of the HIE. *In order to make informed decisions about their health information and to encourage consumer's use of their own data to make health care decisions, they must have access to their data.*
- 10.25.18.03(C)(3) the HIE's responsibility to facilitate the correction of perceived inaccuracies in a patient's health information. *Inaccurate data could be detrimental to consumer health, therefore, one of the top priorities of the HIE, the participating organizations, and consumers should be verifying that all data passing through the HIE is free of errors. HIEs can't correct the data but can direct consumers to the appropriate party to correct inaccuracies.*

**.05 Requirements for Accessing or Disclosing Health Information Through an HIE**

- 10.25.18.05(B) the requirement that information accessed through the HIE be used for the express primary purpose for which the authorized user was given access. *This reassures consumers that their information will be used primarily for treatment and for no extraneous purpose outside the original request.*

**.08 Notice of Breach**

- 10.25.18.08(B) the requirement that the HIE notify individuals of breaches of their data rather than depending on the participating provider to do so is appropriate. *Consumers have a right to know if their data may have been accessed inappropriately, whether this was done by HIE staff, an authorized user, or an unauthorized user. MHAMMD understands this protection creates a new floor above HIPAA, but in order to facilitate a sense of trust in an unfamiliar system, consumers must believe the HIE is consistently acting in their best interests.*
- 10.25.18.08(C) specific requirements for what a breach notification to consumer must entail. *The more specific the information given to consumers about the breach, the more able consumers will be to make decisions and take appropriate measures to protect themselves from repercussions of this breach and to protect from future breaches.*

Again thank you for the opportunity to submit comments. Please contact Adrienne Ellis, 443-901-1550 ext. 206 or [aellis@mhamd.org](mailto:aellis@mhamd.org) with any questions.

**Maryland Health Care Commission**  
**Draft Informal Health Information Exchange Regulations**  
**Comment Form**

Individual/Organization Name: <i>Mental Health Association of Maryland</i> Date: <i>4/29/2013</i>		
Section	Concern	Recommendation
Individual subsections of the draft regulation	Include the organization's concern with the corresponding subsection	Include the organization's recommendation that would remedy the concern raised to the subsection
.01 A Scope		
.01 B Scope		
.01 C Scope	As noted in cover letter, this section conflicts with section .04A(2) which requires "consent or authorization consistent with applicable laws prior to access, use, or disclosure of sensitive information to and through the HIE..." Section .01 C would remove all protections for consumers whose information is exchanged via any point to point transmissions facilitated by the HIE, including education requirements.	Clarify that this exemption applies only to point to point transmissions that occur outside the HIE and have been in no way facilitated by the HIE.
.01 D Scope		
.02 B Definitions	The definition of sensitive health information appears to require both (b)-Part 2 information AND (b) Any other information with specific legal protections...	Replace "and" with "or".
.02 B Definitions	As stated in our previous comments, the definition of consumer which includes the patient and a person in interest is confusing. The use of health care consumer and patient throughout the regulations is duplicative, and the common understanding of the word consumer would not include the person in interest as defined here. Commonly the words consumer and patient would be used interchangeably. The use of all of these terms requires definitions of all three terms that are dependent on each other.	Remove the definition of consumer and use only the definitions of patient and person in interest. Where consumer is used throughout the regulations, "patient and/or person in interest" would be used instead.
.02 B Definitions	In an effort to link as many health care providers as possible through the state designated HIE, the definition of health care provider must be broad enough to include all providers that would be appropriate to serve as participating organizations. There is sometimes confusion as to whether community based rehabilitation or psychiatric rehabilitation programs are considered a facility or institution under Health General 10-101(e).	Clarify that Section 10.25.18.02(B)(15)(b)(i) also includes these providers.
.03 A Consumer Rts		
.03 B Consumer Rts	This section does not address how HIE will make information available to consumers about their sensitive health information in the consumer education plan, which is necessary to ensure consumers are able to make informed decisions about their health care information.	insert into section 10.25.18.03(B)(iii) "specific details correspondent to regulation .04 of this chapter as to who may access, use, or disclose a patient's sensitive health information and for what purpose; and 10.25.18.03 (B) (v) add "including sensitive health information;"
.03 B Consumer Rts	Unlike the previous draft, the section no longer encourages the collaboration of stakeholders in the development of the education plan, which is critical to ensuring that it is culturally competent and consumer accessible.	add 10.25.18.03(B)(1)(c) to read "The health care consumer education plan shall be developed in coordination with interested stakeholders."
.03 C Consumer Rts		
.03 D Consumer Rts		
.03 E Consumer Rts		
.03 F Consumer Rts		
.03 G Consumer Rts	In order to ensure that MHCC can enforce section 10.25.18.03(G), participating organizations must keep record that they have informed patients of their rights as by required 10.25.18.03(G)(1).	rewrite 10.25.18.03(G)(3) to read "A participating organization shall keep record that each health care consumer was informed of:"
.04 A Sensitive PHI	This section needs clarity because as drafted it appears that all mental health records are considered sensitive health information and therefore must be transmitted point to point only. This seems to leave no room for the transmission of sensitive information through the HIE for emergency purposes. It also does not address problems with a participating organizations ability to "flag" a record as sensitive, nor does it allow for a person with a mental health condition to have a complete record available to querying participating organizations. If the regulations are meant to address only the personal/psychotherapy notes as sensitive that must be clarified, but still would leave the problem of how a provider keeps the notes separate from the medical record.	If MHCC did not intend for all mental health records to be considered sensitive and available via point to point transmissions that must be clarified. MHCC must make clear what part of the mental health record has the protections afforded as sensitive health information. MHCC and the HIE Policy Board must consider in further policy discussions issues related to the access, use and disclosure of sensitive health information. For consideration should be whether it is feasible to allow consumers to "opt-in" allowing their mental health or other sensitive information to be included into their complete medical record, as well as whether it is feasible for mental health providers to keep their personal notes separate from the entire, or how a participating organization can "flag" a record as sensitive.
.05 A Access		
.05 B Access		
.05 C Access		
.05 D Access		
.05 E Access		
.05 F Access		
.05 G Access		
.06 A Audit		

.06 B Audit		
.06 C Audit		
.06 D Audit		
.06 E Audit	<p>The posting of an audit summary should not be dependent on request of the Commission. In order to engender consumer trust and to allow for informed decisions about the access, use, and disclosure of their health information, consumers must have access to relevant information about inappropriate access or breaches of information. The audit summary would be publicly available only if a pattern of inappropriate access or disclosure is found, therefore it should not be burdensome to the HIE.</p>	<p>Remove "If requested by the Commission" from 10.25.18.06(E)(3)</p>
.06 F Audit		

.07 A Redial Actions		
.07 B Redial Actions		
.07 C Redial Actions		
.07 D Redial Actions		
.07 E Redial Actions		
.08 A Breach		
.08 B Breach		
.08 C Breach		
.08 D Breach		
.09 A Reg/Enforcement		
.09 B Reg/Enforcement		
.09 C Reg/Enforcement		
.09 D Reg/Enforcement		
.09 E Reg/Enforcement		
.09 F Reg/Enforcement		
General Comments	see attached cover letter	
General Comments		

Meredith L. Borden, Esq.  
Office of the Attorney General

Hi Angela,

Thank you for sharing the new informal draft. I reviewed the January 4, 2012 memo that my office sent to Sondra with our suggested additions to the previous draft of the HIE regulations and was pleased to see that so many of our suggested amendments and additions were included in this draft. I appreciate you taking them into consideration.

I did, however, notice that some provisions we had suggested in our January 2012 memo were not included or at least I could not find them in the new reorganized draft of the regulations. I'd appreciate it if you could point me to where in the new draft regulations the following are, or provide some insight into why the MHCC chose not to include them.

1. Definition of person in interest: We had recommended that the definition of "person in interest" be modified to more fully detail who can speak on behalf of a patient. You included all of the additional clarifying language we had recommended, which we greatly appreciate. However, I could not locate where the language that "'Person in interest' does not mean a participating organization". Did MHCC choose not to include this? If so, why?

2. Audit requirements: In the previous draft of the regulations, we had provided suggested language about what needs to be included in the routine auditing of authentication logs. Specifically, we had suggested that:

.06(B)(1) Audit its authentication logs at least annually to ensure that only an authorized user who is appropriately authenticated is granted access to HIE information through a third party system, including:

- (a) Identifying any findings consistent with the HIE's unusual findings protocol;
- (b) Reporting any unusual finding to the HIE within seventy-two (72) hours of its discovery;
- (c) Determining if the unusual finding constitutes a breach within seventy-two (72) hours of the unusual finding's discovery;
- (d) If the unusual finding constitutes a breach, mitigating the breach promptly;
- (e) Reporting to the HIE the breach's mitigation within twenty-four (24) hours of the mitigation.

I understand that the draft regulations have been reorganized quite a bit. Does the current draft still include a requirement that breaches be mitigated promptly and that the participating organization has to report a breach within 24 hours of mitigation?

3. Large breaches: Similar to HIPAA, we had recommended that if there is a large breach (more than 50 patients) that a public notice of breach be made, including a posting on the HIE's or participating organization's website or in a major print or broadcast media. I couldn't locate this concept anywhere in the new regs. Did the MHCC choose not to include this and, if so, why?

4. Reporting to appropriate authorities: We had recommended in our January 2012 memo that participating organizations and HIEs have an affirmative obligation to report to the appropriate health occupations board when a participating organization or user violated the regulations and/or committed a breach. I see that there is a reporting obligation in .08(D) to the "appropriate federal

and State authorities”. It may be challenging, however, to determine who are the appropriate agencies or if the report to the Commission fulfills this obligations. Is there a reason that this could not say “to the appropriate federal or State authorities, including without limitation the appropriate Health Occupations board”?

Also, because of the rewording of the new draft, I noticed that we had inadvertently forgotten to include in the notice to consumers who had notified the HIE of a potential breach or violation about what happened from that notice. .03(D)(2)(c) includes a notice to the person who filed the notification about what information was breached, but it is possible that no information was actually breached. I think this section would be more complete if it provided that, in response to a written notification about a potential or actual breach, that the HIE shall provide the person and each health care consumer whose protected health information was alleged to be breached or was breached with information concerning the determination and resolution of the matter by the HIE. Therefore, if someone believes that something happened to their PHI, there is an affirmative obligation on the HIE to inform them that something did happen or let them know that nothing did happen.

Finally, in Regulation .09(A)(2)(c), can you provide me with an example of when a bond would not be required? I’m trying to understand why the Commission “may” require a bond under .09(A)(2) rather than “shall” and what circumstances it is trying to account for.

Thank you so much again for all your work on this and for ensuring that consumer protections are included in the draft regulations.

Please let me know if you have any questions about the above or if you want to discuss any of them.

Thanks!

Meredith

Meredith L. Borden, Esq.  
Assistant Attorney General  
Deputy Director, Health Education and Advocacy Unit  
Office of the Attorney General  
200 St. Paul Place, 16<sup>th</sup> Floor  
Baltimore, MD 21202  
(410) 576-6515  
[mborden@oag.state.md.us](mailto:mborden@oag.state.md.us)

VIA ELECTRONIC MAIL TRANSMISSION

April 29, 2013

Angela Plunkett  
Division Chief  
Health Information Exchange  
Maryland Health Care Commission  
4160 Patterson Avenue  
Baltimore, Maryland 21215

Dear Ms. Plunkett:

Thank you for the opportunity to provide comments on the revised draft regulations Chapter 18: Health Information Exchange: Privacy and Security of Protected Health Information. The new draft rules are a very thoughtful and careful revision and we are pleased to see that Part 2 protected information has been specifically addressed in many sections.

We continue to believe, as stated in our prior March 19, 2013 comment letter, that the HIE should be able to develop a mechanism to ensure that Part 2 information is fully accessible and protected in the HIE. However, we accept that, for the initial phase of the HIE and for these initial regulations, only point-to-point transmission of sensitive information will be permitted. As point-to-point transmission will be the only method of providing access to sensitive information, our comments focus on understanding how the point-to-point transmission will be performed, the role of Part 2 programs in the HIE, and how consumer protections, including consumer and provider education, breach identification and notification provisions adequately ensure access to, and provide protection of, Part 2 sensitive information.

Many of our comments are requests for clarification either because we have found what we believe are internal inconsistencies in the draft regulations or because we cannot understand, based on the regulations, how a process works or what entities have responsibility for certain functions. As many of our comments relate to fundamental substantive and process questions and refer to many different sections in the regulation,

**CLINICAL LAW PROGRAM ATTORNEYS:**

Jane F. Barrett  
Barbara Bezdek  
Brenda Bratton Blom  
Patricia Campbell  
Marc Charmatz  
Pamela Chaney  
Douglas L. Colbert  
Jerome E. Deise

Erin E. Doran  
Deborah Eisenberg  
Emily M. Eisenrauch  
Sara Gold  
Toby Treem Guerin  
Terry Hickey  
Kathleen S. Hoke  
Peter Holland

Renee Hutchins  
Sherrilyn A. Ifill  
Andrew W. Keir  
Paige Lescure  
Susan Leviton  
Leigh Maddox  
Rachel Micah-Jones  
Michael A. Millemann

Leslie Turner Percival  
Matthew Peters  
William Piermattei  
Brian Saccenti  
Michelle Salomon  
Maureen Sweeney  
William Tilburg  
Rita Turner

Ellen Weber  
Deborah J. Weimer  
Roger Wolf  
•  
Michael Pinard,  
*Clinic Director*  
A.J. Bellido de Luna,  
*Managing Director*

we have set out in this letter our general comments by subject area which we believe will facilitate your review. In addition, we have included the MHCC comment form which reflects the comments in this letter as well as additional minor comments on identified sections of the draft regulation. To the extent the comment form does not accommodate our entire comment in a legible form, we request that you rely on the full text in this letter.

#### **1. Scope: Application of Chapter 18 to Point-to-Point Transmission**

As a threshold comment on scope, we note that specific reference to 42 C.F.R Part 2 is omitted from Section 10.25.18.01D, which states that the requirements in Chapter 18 are in addition to those under HIPAA and numerous other specifically enumerated federal and state confidentiality laws. Given the importance of Part 2 regulations in understanding the use and disclosure of sensitive information, we suggest that Part 2 should be included in the list of federal and state confidentiality laws specifically identified in subsection .01D.

More importantly, we have found, based on our reading of the regulation, an internal inconsistency in the scope of application of the regulations to point-to-point transmission. Section 10.25.18.01C(2) provides that Chapter 18 does not apply to “The use, access, or disclosure of protected health information using point-to-point transmission.” Point-to-point transmission is defined in Section 10.25.18.02B(33) as a secure electronic transmission that can be read only by the single receiving entity designated by the sender. Section 10.25.18.04A states that, until the Commission develops further rules, “all sensitive information shall only be transmitted via point-to-point transmission.” Taken together, these provisions suggest that point-to-point transmission can occur only outside of the HIE. However, in Section 10.25.18.04A(2) the regulations provide that, where written consent is required by law, persons must “use only point to point transmission to allow access to, use or disclosure of the sensitive health information *through* the HIE” (emphasis added). This provision suggests that, in fact, point-to-point transmission will occur through a transmission process within the HIE. If the HIE will provide the secure linkages for point-to-point and/or will have access to any of the point-to-point transmission information, then the applicable provisions of Chapter 18, including breach and audit requirements, must apply.

A related question arises under Section 10.25.18.03C(1). That provision imposes certain consumer protection requirements relating to “protected information available through the HIE.” Do these consumer protection requirements, including Section 10.25.18.03C(2) that requires the HIE to provide written information to consumers concerning access to the consumer’s health care information, apply to Part 2 sensitive information that is transmitted point-to-point?

Finally, the proposed regulation contains no exception to point-to-point transmission for sensitive information exchange in the event of a medical emergency. Under Part 2, information can be exchanged in the event of a medical emergency without patient consent. (42 C.F.R. § 2.51). Thus, hospitals may transfer records that contain Part 2 information without consent and Part 2 programs may allow access to records in the

event of an emergency. As access to drug treatment information may be critically important in an emergency situation, we request that that exception be made explicit in the regulations and the process and protections relating to emergency access be clearly delineated in the regulations.

## **2. The Role of Part 2 Providers/Programs**

The role of Part 2 programs in the HIE is not specifically articulated in the draft regulations. We assume, based on discussions in the policy board meetings, that Part 2 providers are permitted to be participating organizations. If a Part 2 provider is permitted to be a participating organization, the definition of health care provider in Section 10.25.18.02B(15) should explicitly include Part 2 programs by reference to state certified alcohol and drug treatment programs, consistent with the identification of other health care facilities. In addition, we have identified below several issues that seem to be key to understanding how Part 2 programs may use and access the HIE data.

A. Assuming that a Part 2 program can be a participating organization, how will that relationship be structured in order to comply with Part 2 (apart from the need to enter a business associate/qualified service organization agreement with the HIE)?

i. Will Part 2 program patients who do not opt-out be included in the HIE Master Index? If the Program patients are included in the Master Index, will that information be sufficiently de-identified in order to ensure that it does not constitute patient identifying information as defined under Part 2 (42 C.F.R. § 2.11)?

ii. We assume that the HIE will block access to Part 2 provider records, except for emergencies, as discussed below. The HIE also must ensure that the Part 2 provider is not identified as connected to the patient. Disclosure without patient consent of the fact that the patient has received drug or alcohol program services is a Part 2 violation. (See 42 C.F.R. § 2.12(a)) The HIE mechanism could simply block access or create an indication that there are unnamed providers who hold sensitive information. Such notification would allow the querying entity to request consent from the patient to access appropriate records.

B. Assuming that Part 2 programs can be participating organizations, how will Part 2 records be accessed for emergency treatment purposes? As discussed above, Part 2 permits access to Part 2 protected information in the event of an emergency without patient consent, and drug treatment information may be an important part of any emergency treatment decision-making.

## **3. Part 2 Information within a Record held by a Non-Part 2 Provider**

We are concerned that the draft regulations do not provide sufficient protection and guidance for access to and disclosure of Part 2 information that is part of a record held by non-Part 2 provider. It is our experience that many non-Part 2 providers do not have the technical capacity or sufficiently complete understanding of Part 2 to fully and appropriately ensure that Part 2 information in a patient record is re-disclosed only as

permitted under Part 2.

The draft regulations place the responsibility for identifying and protecting sensitive information solely on the participating organization, and we are pleased to see that the HIE oversight responsibilities, including breach responses and audits, relate to use and disclosure of sensitive information. However, it is unclear to us how the process for identifying sensitive information occurs. If a provider has sensitive information, what are the mechanisms for alerting the inquiring entity that some information is sensitive and would require point-to-point transmission? If the obligation to identify and protect sensitive information falls to the participating organization, the regulations should specifically require those participating entities to disclose the existence of sensitive information in a way that complies with applicable law, including Part 2. The existence of Part 2 information cannot be revealed by the participating organization without patient consent. (See 42 C.F.R. § 2.12(a)).

#### **4. Consumer and Provider Education.**

Consumer education relating to Part 2 protections generally and under the HIE will be an important component of the consumer protections in the HIE. As noted above, not all non-Part 2 providers are adequately informed about Part 2 requirements. HIE Core education must include significant education on Part 2 requirements, the scope of sensitive information subject to the HIE regulations and the specific protections and limitations for access to and use and disclosure of sensitive information under the HIE. For the consumer, education and information about the use and disclosure of sensitive information is a key component of the information needed to make an informed decision on the consumer's opt-out option. One of the important components of the education must include information on the scope of a non-HIPAA breach and breach notification for sensitive information.

#### **5. HIE Role as Qualified Service Organization in Oversight, Audit and Investigation Functions under .06 and .07**

Regardless of whether sensitive information flows outside or through the HIE, the HIE will have access to Part 2 information in its oversight and audit functions. The HIE's access of this Part 2 information could constitute an unauthorized disclosure unless the HIPAA business associate agreement between the HIE and participating organization meets the additional requirements that apply to qualified service organizations under 42 C.F.R. § 2.11. (See also 42 C.F.R. § 2.12(c)(4)). We recommend that, in order to ensure that disclosures to the HIE comply with Part 2, Section 10.25.18.05A(3) specifically require that all business associate agreements between participating organizations and the HIE include the required Part 2 QSOA provisions. In addition, a definition of "qualified service organization" should be added to Section 10.25.18.02 (consistent with the definition of "business associate") and incorporate the meaning as defined in 24 C.F.R. § 2.11.

In addition, the regulations provide for certain oversight and remedial functions to be performed by the Commission. For example, in Section 10.25.18.07C(2), the HIE must provide to the Commission a copy of any finding related to a non-HIPAA breach. If that information provided to the Commission includes patient identifying information, Part 2 would require compliance with 42 C.F.R. §2.53 relating to audit and evaluation activities. Section 2.53 requires that the Commission and the HIE (on behalf of the provider) enter into an agreement relating to maintenance, re-disclosure and destruction of the Part 2 information.

## **6. Breach and Breach Notification**

We appreciate the importance and challenges of providing for different responses to HIPAA breaches and non-HIPAA violations, and we have spent considerable time parsing through the draft regulation in an effort to understand the various requirements relating to breach and non-HIPAA breach notification. In our view, the regulations are inconsistent and unclear as to the non-HIPAA violation notification obligations of the HIE and the Participating Organizations. We have identified below the specific issues and inconsistencies relating to breach notification and have also offered specific recommendations for the HIE to consider in clarifying and expanding the respective responsibilities. In addition, we have recommended consideration of a separate standard for content and communication of non-HIPAA violation notifications in order to ensure full protection of sensitive information, including Part 2 information.

### **A. Clarify the circumstances that give rise to an HIE obligation to provide notice of a non-HIPAA violation.**

Section 10.25.18.08(B) of the draft regulation provides that, “[w]hen federal or state law does not require an HIE or other entity to provide notification to a participating organization or to an affected health care consumer, or *when Part 2 does not mandate other notification requirements*, the HIE shall provide notification of breach and, if applicable, non-HIPAA violations pursuant to this chapter.” (emphasis added).

We are unaware of any mandatory notification obligations under Part 2 and would like clarification as to the meaning and intent of this reference. In addition, it would be helpful to clarify what federal or state notification requirements other than HITECH might exist that would relieve the HIE of its obligations under this notification section.

### **B. Role of the HIE and the Participating Organization for Notification of a Non-HIPAA violation.**

#### **1. Role of the HIE**

Section 10.25.18.08B provides for HIE notification only if there is no notification under other specified laws. However, .08B(1) states that the HIE “shall” notify various recipients if an investigation under .07 concludes there is a breach. It would be helpful to clarify the parameters of the HIE obligation.

## 2. Role of Participating Organizations

Draft regulation Section 10.25.18.08B requires the HIE to report all non-HIPAA violations; however, Section 10.25.18.03G(2) requires all Participating Organizations to notify consumers of breaches of information, including sensitive health information, consistent with HIPAA and Regulation .08.

We read Section .03G(2) to provide that Participating Organizations must report all breaches, including any breach of sensitive information that is a non-HIPAA violation, in accordance with HIPAA breach notification rules. This would expand the HITECH notification rules that govern Participating Organizations to apply to non-HIPAA breaches. We would support this expansion of the HITECH breach notification rules with the added protections for sensitive information that we discuss below.

However, it is also possible that the intent of Section .03G(2) is to require Participating Organizations to report HIPAA breaches only as required under HITECH rules. We note that under Section 10.25.18.08A, Participating Organizations *only* have an obligation to report as required under HIPAA and HITECH. This reading would remove the responsibility for reporting serious privacy violations from the Participating Organizations that engaged in the violation and potentially undermine the remedial/corrective goal of such notification obligation.

We suggest that Participating Organizations should also have a responsibility to give notice to consumers for breaches and non-HIPAA violations that are identified as violations by the HIE (or the organizations' own audit). Specifically, we recommend that Participating Organizations identified in an investigation as responsible for a non-HIPAA or HIPAA violation also have responsibility for giving notice to affected consumers for HIPAA and non-HIPAA breaches. We note that there will be some HIPAA breaches that the risk test, will not require notification to the consumer and yet will trigger an HIE notification under the draft regulation. In our view, to the extent such breaches occur in the HIE and are identified under a .07 investigation as a breach or violation, those breaches or violations should also be reported to the consumer by the responsible Participating Organization.

### **C. Content and Means of Communication for Sensitive Information Breach Notification**

In the structure proposed under the draft regulations, there is clear recognition of the heightened risk for the consumer in inadvertent disclosure of Sensitive Information and the importance of establishing special protections for Sensitive Information. In our view, heightened protections should also apply to the notification provisions relating to Sensitive Information. We have proposed below two additional protections relating to the content of the notification and the means of communication that we believe provide additional and needed protections for Sensitive Information.

## **1. Content of Notification**

Section 10.25.18.08C(5) sets out the required content for a breach notification; however, the regulation does not impose any limits on the scope of information that might be contained in the “description of the breach or non-HIPAA violation that occurred and the remedial actions taken...” (Section 10.25.18.08C(5)(a)). Without more prescriptive guidelines, we believe that Section 10.25.18.08C(5)(a) would permit a notification to include Sensitive Information, including Part 2 information. Although there is no Part 2 requirement that explicitly addresses or limits breach notification, we are concerned that notifications that identify Part 2 information present a risk of inappropriate disclosure of sensitive information in the event such notification is errantly sent or received or intercepted. We recommend adding a requirement that the notification of non-HIPAA breach or HIPAA breach by the HIE shall not include Sensitive Information.

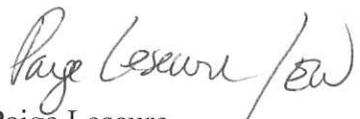
## **2. Method of Notification.**

Section 10.25.18.08C(2) offers only two means of breach notification: (i) In writing by first-class mail; or (ii) If specified as a preference by the health care consumer, by electronic mail. We are concerned that these limited options do not adequately ensure security of Sensitive Information. HHS has recognized the need to provide special protections in breach notifications for highly confidential treatment services. In the preamble to the final HITECH rules, HHS creates discretionary exceptions to the HITECH law requirement for written breach notice and permits individuals to affirmatively elect to communicate orally or by telephone or to be notified of the opportunity to collect a breach notification at the provider’s office. 78 Fed Reg.5566, 5651 (January 25, 2013).

In our view, the HIE breach function should incorporate at a minimum the same consumer protections that are available under the HITECH rule and the draft regulation should permit individuals to specify a preference for the manner of receipt for notifications that relate to Sensitive Information. The draft regulation already establishes alternative means of communication under Section 10.25.18.03F(1) that permit consumers to specify a preference for receiving general communications with the HIE on participation status, including first class mail, electronic mail, phone, fax, online, or in person. For these reasons, we recommend that the HIE regulation permit consumers to affirmatively elect to receive breach communications relating to Sensitive Information by all mediums identified under Section 10.25.18.03F(1).

Thank you for considering our views. We look forward to working with you to develop a comprehensive set of regulations that will address the unique regulatory protections afforded the health records of individuals who have participated in alcohol and drug treatment. Please feel free to contact Ellen Weber at [eweber@law.umaryland.edu](mailto:eweber@law.umaryland.edu) (410-706-0590) if you have any questions or need additional information.

Sincerely,



Paige Lescure  
Senior Health Law & Policy Fellow



Ellen Weber  
Professor of Law



Ian Clark\*  
Student Attorney



Brian Newman\*  
Student Attorney

\* Practicing Pursuant to Rule 16 of the Maryland Rules