*M*emorandum

To: Commissioners

From: David Sharp, Director of the Center for Health Information Technology

Date: October 17, 2013

Subject: Recommendation for Proposed Regulations: ***COMAR 10.25.18, Health Information Exchange: Privacy and Security of Protected Health Information***

Background

Staff seeks Commission adoption of COMAR 10.25.18, Health Information Exchange: Privacy and Security of Protected Health Information, as proposed permanent regulations. These regulations result from House Bill 784, *Medical Records – Health Information Exchange* (HB 784), signed into law on May 19, 2011. The law, Md. Code Ann., Health-Gen. §§4-301 and 4-302 (2011), requires MHCC to adopt regulations for the privacy and security of protected health information obtained or released through a health information exchange (HIE).

In the spring of 2012, MHCC released an informal draft of the HIE regulations and received over 33 informal comment letters. In general, comments from providers and HIEs stated that the requirements would be burdensome to implement, and some consumers expressed preference for tighter controls over the data that flows through an HIE. On March 14, 2013, a second informal draft was released. Staff received written comments from 18 organizations and individuals, including:

- Accountable Care Organizations of Maryland (ACOs of Maryland)
- American Civil Liberties Union of Maryland (ACLU-MD)
- British American Auto Care
- CareFirst BlueCross BlueShield (CareFirst)
- Chesapeake Regional Information Systems for Our Patients (CRISP)
- Coventry Health Care of Delaware, Inc. (Coventry)
- FUSE Health Strategies: Consulting group specializing in behavioral health policies
- Jennifer Thomas, PharmD. (Dr. Thomas)

- Johns Hopkins Health System Corporation (JHHS)
- Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. (Kaiser)
- Koss on Care, LLC
- Mary Jo Deering, Ph.D. (Dr. Deering)
- Maryland Hospital Association (MHA)
- Maryland Institute for Emergency Medical Services Systems (MIEMSS)
- Mental Health Association of Maryland (MHAMD)
- Maryland Office of the Attorney General, Consumer Protection Division (OAG-CPD)
- University of Maryland School of Law

Staff Recommendation

Staff recommends that the Commission adopt COMAR 10.25.18 as proposed permanent regulations.

Summary of Key Comments and Staff Action

Staff completed a thorough review of more than 120 individual comments received from 18 individuals and organizations. The remainder of this document addresses key substantive comments and includes staff action. A complete set of the written comments received on the informal draft HIE regulations is attached for your reference.[1]

Scope and Exemptions

- ACOs of Maryland recommended including in Section .01C an exemption of an exchange of protected health information (PHI) between an ACO and a participating organization. Additionally, CareFirst recommended that the same exclusion that applies to hospitals should also apply to payors

  Staff action – No change: While the exchange of PHI between a hospital and its medical staff is exempt from the regulation, staff believes that the exchange of PHI between an ACO and its participating organization or a payor and network providers should not be excluded from compliance with the regulations as these

[1] A complete set of the written comments received on the draft regulations may be obtained electronically here: http://mhcc.dhmh.maryland.gov/hit/hie/Documents/informal_comments.pdf.

exchanges typically occur between entities not under common ownership or where employment is involved.

- The ACLU-MD suggested that the scope and purpose of the regulations, as detailed in Section .01, specify that this chapter addresses the privacy and security of "health information and information derived or obtained from, or based on protected health information obtained or released through an HIE."

  Staff Action – No change: Health-General Article §4-302 related to these proposed regulations gives MHCC the authority to "adopt regulations for the privacy and security of protected health information" and not all health information.

- Koss on Care noted that the regulations do not address the interoperability of HIEs. Koss on Care recommended that the regulations specify requirements for certain entities to exchange with the State-designated HIE, which would support the goal of patients being able to access their information wherever it resides throughout the state.

  Staff Action – No change: Health-General Article §4-302 related to these proposed regulations provides that MHCC "may adopt regulations for implementing the connectivity to the State-Designated exchange...." Staff believes that such regulations are not needed at this time.

- The ACLU–MD recommended that a payor-operated HIE should not be authorized until further consideration is given to the requirements for payor-operated HIEs by the HIE Policy Board.

  Staff Action – No change: Health-General Article §§4-301 and 4-302 related to these proposed regulations allows for the operation of a payor-operated HIE.

- The ACLU-MD, CareFirst, Coventry, the MHAMD, and the University of Maryland School of Law, recommended that MHCC clarify when point-to-point exchange of information would not fall within the scope of the regulations.

  Staff action – Change made: The proposed regulations do not intend to place additional requirements on certain electronic transaction that involve PHI where the exchange is occurring via a secure message for a single sender to be read only by a single receiver, such as secure email. However, when an HIE is involved in the transmission of the message, the regulations apply. Changes were made to Section .01C(1) to clarify.

- CRISP, Coventry, and Dr. Deering raised concerns with the definition of an HIE within Section .02B(17).

Staff action – Change made: Maryland law, Health-General Article §4-301 initially defines an HIE; the proposed definition intends to clarify the definition further. The proposed regulations, and Maryland law, regulate HIEs that maintain, whether or not they actually create, an infrastructure that provides for the electronic exchange of PHI. For this reason, "or maintains" was added to provide clarification.

- The MHAMD recommended that health care providers, as defined in Section .02B(15) include psychiatric rehabilitation. Dr. Thomas also recommended that pharmacies and pharmacists be included in the definition of a health care provider.

  Staff action – No Change: Staff believes that the references within the definition to the Health-General Article and the Health Occupations Article include these providers.

Consumer Rights

- The ACLU-MD raised concerns regarding the rights of minors and suggested that, until further consideration is given regarding these rights, the regulation should explicitly exclude minors between the ages of 10 and 18 from the HIE.

  Staff action – No change: Staff believes that current laws regarding the rights of minors around the use and disclosure of their PHI are sufficient and would apply to the electronic exchange of PHI through an HIE.

- Dr. Thomas recommended that an additional exception be added to allow disclosures through the HIE even if a patient opts out for results of prescription medications filled by a pharmacy and disclosed to the health care provider who ordered the prescription.

  Staff action – Change made: Exceptions for opt out are intended to allow certain electronic transitions that are currently occurring to continue without additional restrictions. Staff agrees that prescription medication fill history to the ordering provider should be an exception to opt-out, just as the results of a procedure to the ordering provider are allowed even in the event that a patient opts out. Proposed language added to Section .03A(2)(a)(iv).

- CRISP recommended that certain direct communications between physicians, which are the functional equivalent to faxing or secure email, should be permissible even when a patient opts out. CRISP also noted that certain direct messages that are automated may necessitate giving patients the right to opt-out

  Staff action – Change made: Staff agrees that certain direct communications should be allowed without additional restrictions and proposed language in Section .03A(2)(a)(vi).

- Kaiser suggested that clarification around the opt-out exemption in the event of "Federal or State law requirements."

  Staff action – Change made: Staff agrees and included proposed language to Section .03A(2)(a)(ii) to clarify that these include disclosures,"that a person is required to make under federal or State law requirements."

- Coventry requested clarification regarding what entity is required to provide notification, as detailed in Section .03A(2)(c), to a consumer regarding details of a patient's opt-out status.

  Staff action – No change: Staff believes that the regulation specifically identifies the HIE as the responsible entity in the following language: "A health care consumer shall be advised in writing by the HIE...."

- Koss on Care noted that a health care consumer should be provided with the ability to access their health information through a single point of access and recommended that HIEs and participating organizations be required (over a phased-in time period) to offer health care consumers a single point of access to their information across health care providers

  Staff action – No change: Staff agrees that such access is important to patients and recommends that policies specific to these types of requirements be considered by stakeholders prior to establishing this requirement.

- The MHAMD recommended that the regulations require an HIE to work in coordination with stakeholders to develop and implement a health care consumer outreach and education plans as detailed in Section .03B.

  Staff action – Change made: Staff agrees that an HIE should seek input from stakeholders in the development and implementation of a consumer outreach and education plan and has added language to Section .03B(1).

- CareFirst raised concerns regarding consumer rights as detailed in Sections .03C, .03B, .03G, and .03F.

  Staff action – No change: Staff believes that the regulation appropriately balances the rights of consumers, regarding the privacy and security of their health information, and the efficiency of HIE operations.

- The ACLU-MD recommended that the regulation specify that a participating organization obtain assent prior to making a query through the HIE.

Staff action – No change: Staff believes this requirement would cause an undue burden on providers.

- CRISP noted that the regulations require HIEs to provide certain information to a health care consumer describing what PHI is available through the HIE as detailed in Section .03C(1). CRISP recommended that the regulation specify that only information being disclosed via a query to the HIE should apply in these cases, and not those being transmitted by the HIE via point-to-point, as the HIE would not have records related to disclosures made via point-to-point.

  Staff action – Change made: Staff agrees that the regulations specify that an HIE is required to provide certain information to a health care consumer in the event that a patient's PHI is disclosed to the HIE. The type of PHI disclosed to the HIE, as detailed in Section .03C(1)(c) should only be provided if accessible to the HIE. Language was added to Section .03C(1)(c) and Section.03C(4)(b)(iv).

- Koss on Care and British American Auto Care recommended that health care consumers be allowed to provide a notice or request to an HIE via a website or email.

  Staff action – Change made: Staff agrees that health care consumers should have options when making requests of an HIE, such as when a health care consumer requests an accounting of disclosure made by the HIE. Staff has included proposed language within Section .02B(25) to allow notices and requests to be provided to and from an HIE or participating organization via specific electronic or digital mechanism under certain circumstances.

- The ACLU-MD suggested that an HIE provide information to the health care consumer about how to correct perceived inaccurate information being made available through the HIE in 10 days, rather than 30 days upon receipt of notice of a perceived inaccuracy as detailed in Section .03C(3)(a).

  Staff action – Change made: Staff believes that 20 days will allow an HIE to provide such information. Language within Section .03C(3(a) was added.

- The MHA noted that a health care consumer should contact the specific provider that originated the data if they believe an inaccuracy exists.

  Staff action – No change: Staff believes that including a requirement on health care consumers to contact their specific provider is out of the scope of this proposed regulation. The proposed regulation, as detailed in Section .03C(3), requires action to be taken by an HIE in the event a health care consumer notifies the HIE regarding a perceived inaccuracy.

- CRISP recommended that the regulations specify a procedure in Section .03C(4) to allow an HIE to provide a summary report of disclosures to a health care consumer in cases of recurring disclosures by the HIE to the same entity for the same purpose.

  Staff action – Change made: Staff agrees that an HIE should be allowed to provide summary reports in cases of recurring disclosures, and that an HIE should be required to provide details of the summary report, if requested by a health care consumer. Language was proposed in Section .03C(4).

- The ACLU-MD noted that the regulations should clarify in Section .03G(1) a timeframe and method by which a participating organization is required to notify each health care consumer regarding their participation in an HIE, the consumer's right to opt out from participating in the HIE, and the process to opt out. The ACLU-MD recommended that this notice be provided no later than the first medical encounter with the patient following enrollment of the organization in an HIE by written and oral notice.

  Staff action – Change made: Staff agrees and language was added.

- Coventry requested that the regulations specify what information is must be tracked by the HIE and what information must be tracked by a participating organization in Section .03D(1) as it would impact auditing.

  Staff action – No change: Staff believes that Section .03D(1) is intended to generally address the requirements on an HIE to protect a patient's PHI from a breach or violation of this chapter. Section .06 specifically addresses the auditing requirements for both an HIE and participating organization specifically.

- CareFirst raised concerns with the requirements related to user authorization as detailed in Section .05E.

  Staff action – No change: Staff believes the regulations provide HIEs with appropriate flexibility in implementing the requirements while assure protection of electronic health information.

- Coventry recommended that an HIE be provided with 10 business days, rather than five, to implement the health care consumer's request to opt-out or opt back into the HIE, as detailed in Section .03F(4).

  Staff action – No change: Staff believes that five business days is appropriate.

- Kaiser suggested that participating organizations should be allowed to provide notice regarding their participating in the HIE and the patient's right to opt-out on their website, rather than in writing, as detailed in Section .03G(1).

Staff action – No change: Staff believes that written and oral notice is important to inform patients regarding their right to participate or not in the exchange of PHI through an HIE.

- Dr. Deering noted that the regulations, as detailed in Sections .03A(2) and G(1)(b), do not clearly indicate what the mechanism is for opting out; i.e., if the health care consumer may opt-out at the individual provider level or the HIE level, and whether both the participating organization and HIE communicate to the health care consumer about the right to opt-out. The ACLU-MD also recommended that the regulations allow for an HIE to operate under an opt-in basis.

  Staff action – No change: The proposed regulations are silent on the level at which a patient may opt-out. Opting out at an individual provider level is not prohibited by these proposed regulations. Further, the regulations do not prohibit an HIE from operating under an opt-in basis. Additionally, the proposed regulations required the HIE to develop and implement an education plan for health care consumers, as detailed in Section .03B(1), and specific written and oral notice must be provided by the participating organization regarding a patient's right to opt out, as detailed in Section .03G(1). Staff believes that a coordinated effort is important. However, specific notice by a participating organization has the potential to be more effective than notice from an HIE.

- CRISP suggested that the regulations specify a procedure in Section .03F(2) to allow a health care consumer to communicate regarding opting out or opting back into an HIE via telephone.

  Staff action – Change made: Staff agrees that a health care consumer should be allowed to opt out or opt back into an HIE via telephone; however, a written confirmation must be provided by the HIE to the health care consumer. Language was added to Section .03F(2).

- Kaiser noted that an HIE should be required to "send" rather than "provide" confirmation to a health care consumer regarding certain requests, such as a request to opt-out or opt back in to the HIE.

  Staff action – Change made: Staff agrees and changed "provide" to "send" in Section .03C(3)a and F(5)a, and Section .07F(1).

Sensitive Health Information

- FUSE Health Strategies and the MHAMD suggested that the regulations explicitly state that an HIE must provide to health care consumers, as part of its outreach and education plan, details concerning who may access, use, or disclose a patient's health information, "including sensitive health information" in Section .03B(1)(b)(iii). The

University of Maryland School of Law raised a similar concern regarding a patient's right to information about what sensitive health information is made available through an HIE in Section .03C(1-2).

Staff action – Change made: Staff believes that sensitive health information should be included as part of health information detailed in Section .02B(16); therefore, staff added language within the definition of protected health information to include "a subset of health information..." in Section .02B(36).

- The MHAMD commented that the definition of sensitive health information in Section .02B(40) should include *Part 2 information* "or" *any other information that has specific legal protections*..., rather than "and."

Staff action – Change made: Staff agrees and changed the language within the definition of sensitive health information from "and" to "or."

- JHHS recommended that the regulations explicitly clarify that disclosures of sensitive health information should not apply to certain disclosures allowed when a patient opts out.

Staff action – Change made: Staff agrees and changed the language within Section .03A(2)b to clarify that certain disclosures that may occur even if a patient opts out should not apply if sensitive health information is to be disclosed.

- FUSE Health Strategies noted that the requirements in the draft regulations, which limit the exchange of sensitive health information to only point-to-point exchange, prevent patients with mental health and substance abuse disorders from realizing the benefits of HIE. FUSE Health Strategies recommended that MHCC consider using policies similar to Rhode Island and the guidance provided by the Substance Abuse and Mental Health Services Administration (SAMHSA). MHA also noted that only using point-to-point for the exchange of sensitive health information would be technically challenging. CareFirst recommended that the regulations allow for the exchange of sensitive health information in other ways besides point-to-point. Koss on Care noted that the requirements around the exchange of sensitive health information are unclear.

Staff action – No Change: Staff believes that there are technology limitations around adequately protecting electronic sensitive health information consistent with the guidance provided by SAMHSA. To ensure that electronic sensitive health information is appropriately safeguarded, staff concludes that limiting the electronic exchange to point-to-point is necessary at this time. Staff will continue to monitor advances in HIE technology and expects that in the not-too-distant future HIEs will be able to exchange sensitive health information.

- FUSE Health Strategies recommended that the regulations specifically address re-disclosure of records that are incorporated into the patient's medical record.

  Staff action – Change made: Staff agrees and added language within Section .05A(4) to clarify that authorized users must comply with all applicable federal and State laws regarding re-disclosure of medical records.

Implication of Part 2

The University of Maryland School of Law raised several concerns with the implications of the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations as detailed in 42 CFR § Part 2 (Part 2) and the proposed regulations. Part 2 applies to federally assisted substance abuse treatment programs and requires additional protections with regard to the use and disclosure of information related to the records of patients treated by such programs. The key comments below are provided by the University of Maryland School Of Law regarding Part 2.

- Expressed concerns that information in the Master Patient Index for Part 2 program patients that do not opt-out should be sufficiently de-identified.

  Staff action – No change: Staff believes that current technology is not capable of performing separation of Part 2 program patient information. Staff will monitor technology development to determine an appropriate time to revise this requirement.

- Requested that Part 2 be included within the list of privacy and security laws under Section .01D that are in addition to the requirements purposed by this regulation

  Staff action – Change made: Staff agrees and added language to Section .01D(6).

- Recommended that Part 2 treatment programs be included within the definition of health care provider in Section .02B(15).

  Staff action – Change made: Staff agrees and added language to the definition to include a State-certified alcohol and drug treatment program, as defined in Health-General Article §8-403.

- Noted that an HIE should be required to include Part 2 provisions in all Business Associate agreements, as detailed in Section .05A(3).

  - *Staff action – Change made: Staff agrees and added language to require that HIEs include Part 2 provisions in all Business Associate agreements where the participating organization will maintain Part 2 information.*

- Raised concerns around including Part 2 information within the notice to certain entities when an HIE has reasonable belief that a breach or violation has occurred as detailed in Section .07C(2)a. They noted that if such notice, specifically within a copy of the findings of the investigation, included certain patient information, the notice must be provided in compliance with Part 2.

  Staff action – Change made: Staff agrees that the regulations should clarify that these types of notices should exclude sensitive health information and added language to Section .07C(2)a.

- Noted that the regulations do not provide sufficient protection and guidance for disclosure, re-disclosure, and maintenance of Part 2 information by non-Part 2 providers.

  Staff action – Change made: Staff agrees that the regulations should clarify procedures around disclosure, re-disclosure, and maintenance of Part 2 information by non-Part 2 providers and added language to Section .04B.

- Recommended that the regulations permit Part 2 information to be accessed without consent in a medical emergency as Part 2 allows for such access.

  Staff action – Change made: Staff agrees that the regulations should align with current laws around Part 2 when feasible and added language to Section .04A(3) regarding the access of Part 2 information in medical emergencies.

- Suggested that the notification, as detailed in Section .08, should include two additional protections regarding Part 2 data.

  Staff action – No change: Staff believes that the regulations are consistent with State and federal law.

User Access to Health Information

- JHHS recommended that research and all health care operations be included as a primary use, as defined in Section .02B(35). FUSE Health Strategies suggested that the primary use definition include the use of PHI for generalizable knowledge.

  Staff action – No Change: Staff believes that research, the use of health information for generalizable knowledge, and certain health care operations should not be considered a primary use as it may require patient consent or additional deliberation is needed prior to allowing for these uses through an HIE. Additional consideration for the requirements around secondary use of data will

be made by the stakeholders and may be included in future amendments to these regulations.

- The MHAMD recommended that the regulations, in Section .05B, specifically only allow for the use of information for the purpose for which the information was accessed through the HIE.

  Staff action – No change: Staff believes that the request is outside the scope of the regulations.

- Dr. Deering questioned how the HIE will have assurances that a third party system is compliant with the regulations and all applicable federal and State privacy and security regulation, as detailed in Section .05E(5).

  Staff action – No change: The proposed regulation allows for an HIE to accept a third party system's authentication of an authorized user accessing the HIE through a third party, for example if a user were to access the HIE through their electronic health record system. Staff believes the regulation sufficiently provides in Section .05E(5)(b) that the HIE must obtain "written assurances from the third party system that it is compliant with these regulations and all applicable federal and State privacy and security regulations."

- CareFirst recommended that the regulation specify that access to the HIE be terminated when an authorized user no longer requires access to the HIE.

  Staff action – Change made: Staff agrees and added proposed language within Section .05G(5)(c).

- Dr. Deering suggested that the regulation, in Section .05G(5), specify the party required to notify the system administrator when a user's access should be terminated, including the timeframe.

  Staff action – No change: Staff believe that this level of specification is not needed, as the proposed regulation requires a system administrator to be the responsible person who is required to immediately terminate a user's access under certain circumstances.

- CRISP noted that system administrators should not collect authorized users' passwords.

  Staff action – Change made: Staff agrees and has made the change in Section .05G(1).

- CRISP suggested that the regulations not require a confidentiality agreement with all HIE contractors' staff for disclosures for daily operations and maintenance, as detailed in Section .02B(3). They noted that this will be difficult to implement as to the staff of a contractor, which may change over time and is not under the direct supervision of the HIE.

  Staff action – Change made: Staff agrees and made changes to Section .02B to allow access to contractor's staff, but only if the HIE has a Business Associate agreement with the contractor and the contractor has contractually agreed to limit access to the HIE only to its employees, agents, and independent contractors, with a need-to-know and who are under confidentiality restriction, which may include a binding work force policy and procedure.

- The ACLU-MD stated that the definition of "primary use of HIE data" within Section .02B(35) is too broad, as it allows for additional unintentional uses of information through the HIE that are "permitted by law including those set forth in Health-General Article, §4-305(b), Annotated Code of Maryland"

  Staff action – Change made: Staff agrees that clarity is needed to ensure that the definition does not allow for certain uses of PHI through the HIE and added proposed language to Section .02B(35) to indicate that such uses must also be in accordance with this chapter.

- Kaiser and the ACLU-MD recommended clarification around the opt-out requirements. Both noted that if HIEs are restricted from disclosing PHI if a patient has opted out, including secondary use, except as otherwise permitted under applicable law, as detailed in Section .03E(3), then the regulation would allow for additional unintentional use of information through the HIE.

  Staff action – Change made: Staff agrees that further clarification is needed and included language in Section .03E(2) to indicate that such disclosures must also be in accordance with this chapter.

- CRISP noted that the regulations, as detailed in Section .03E(3), do not allow for disclosures of de-identified data derived from a patient's PHI when the patient has opted out, and recommended that the regulations permit the HIE to disclosure de-identified data even if a patient opts out when the information is part of a count; e.g., when CRISP provides hospitals with a count of statewide readmission for the prior month. CareFirst also noted that the HIEs should be able to use de-identified data of patients who have opted out.

  Staff action – No change: Staff believes that certain uses of de-identified data are considered secondary use. Staff recommends that further consideration

regarding the requirements of secondary data use be taken by stakeholders prior to detailing requirements. However, the regulations as detailed in Section .03E(3) specify that, if permitted under applicable law, an HIE may disclose information derived from a patient's PHI, including for secondary use even if the patient has opted out.

- Koss on Care raised concerns with the requirements around secondary data use and the definition of secondary data use. Koss on Care indicated that the examples provided under the definition in Section .02B(39) raise great cause for concern for many individuals and recommended a broader, less biased set of examples be included. Additionally, Koss on Care stated that the allowable secondary uses, as detailed in Section .04C, are very broad categories of information, and recommended that some aspects of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security rules (45 CFR §§160 and 164) should be reiterated and some preference for use of limited data set and IRB approval of the need for identifiable data should be included.

  Staff action – No change: Staff believes that more consideration concerning secondary data use is needed prior to permitting additional secondary uses. The allowable secondary uses detailed in Section .04C are intended to broadly coincide with certain health care operations that are allowable under HIPAA.

- CareFirst recommended clarification around the requirements for disclosures made to participating organizations and how the HIE would only disclose information where the participating organization may incorporate the information into the organization's EHR, as previously detailed in Section .05B(2).

  Staff action – Change made: Staff believes that the draft language was intended to provide guidance to participating organizations and made changes to specify that the HIE may only disclose patient information in accordance with these regulations.

- The ACLU-MD, the OAG-CPD, Kaiser, and Koss on Care raised concerns with the requirements around secondary use of data as detailed in Section .05C.

  Staff action – No change: Staff is working with stakeholders to identify policies for secondary uses of data that will be considered when staff drafts regulations concerning secondary use.

Audits, Transparency, and Breach

- The MHA noted that unusual findings should be handled in the same manner as a potential breach, as detailed in Section .06.

Staff action – No change: Staff believes that requiring HIEs to address unusual findings in the same manner as a potential breach would create an unnecessary burden on HIEs.

- Coventry requested that the regulations in Section .06A specify if an audit across systems is required, as member information may flow through many different systems.

  Staff action – No change: Staff understands that each HIE may have different systems that make up its infrastructure. The regulations allow for HIEs to implement appropriate "protocols, methodologies and a monitoring approach" when performing an audit, and provide that the approach must be "performed in accordance with best practices using industry accepted standards and methodologies.

- CareFirst recommended that the regulations in Section .03D(2)(c) only apply if a breach is confirmed.

  Staff action – No change: Staff notes that the proposed regulations specify that notice of a breach is provided to "each health care consumer whose protected health information was breached...."

- Kaiser and the MHA raised concerns with the concept of a "non-HIPAA violation" as detailed in Section .02B(25) and Sections .03D and .08B.

  Staff action – No change: Staff believes that the regulations are appropriately ensured that an HIE addresses potential user violations and implements best practices regarding the use of PHI.

- CareFirst noted concerns regarding the requirements for HIEs in developing and implementing protocols to use when auditing the user authentication logs, as detailed in Section .06A.

  Staff action – No change: Staff believes that the regulations provide appropriate flexibility to allow HIEs to develop and implement protocols.

- Koss on Care noted that the regulations are unclear in Section .06C and .06D, as to whether a third party auditor is required.

  Staff action – No change: Staff believes that the regulations indicate that a third party auditor shall be utilized, "at the request of the Commission."

- The OAG-CPD recommended that a health care consumer be notified in the event of a potential breach. The ACLU-MD also recommended that a health care consumer be notified whenever there is reasonable belief of a breach or violation of this proposed chapter, as detailed in Section .07C(4).

  Staff action – No change: Staff believes that notice to a health care consumer should be provided when an actual breach has occurred, as detailed in Section .03D(2)(c) and Section .07C(4). Notification of potential breaches may result in unnecessary actions and time spent by HIEs and/or by health care consumers when no breach is later found.

- FUSE Health Strategies suggested that the regulations specify a minimum number of patients (not records) that must be involved when an HIE or participating organization conducts an audit of its user authentication logs for improper access use or disclosure, or the regulations should specify a percentage of patients that must be involved.

  Staff action – Change made: Staff believes that each HIE should be required to develop and implement protocols, methodologies, and a monitoring approach for conducting audits of its user authentication logs using industry acceptable standards and methodologies. Language to clarify this was added to Section .06A(1-2).

- The OAG-CPD recommended that the regulations should specify that, during a routine audit of authentication logs, the participating organization must determine if an unusual finding constitutes a breach within 72 hours of discovery of an unusual finding and report to the HIE the breach's mitigation within 24 hours of the mitigation.

  Staff action – No Change: Staff believes that the proposed regulation requirements are sufficient.

- FUSE Health Strategies stated that an HIE should always be required to post a summary report of its audit (when a breach or violation was found) on its website, not just at the request of MHCC, and that MHCC should be required to also post the report on its website.

  Staff action – Change made: Staff agrees that transparency regarding the result of certain audits is important and made changes to Section .06E(3).

- FUSE Health Strategies recommended that, in cases where a participating organization does not conduct its own audit, the participating organization should be required to review the HIE provided authentication logs within 10 days of receipt and

that the HIE should provide the authentication logs quarterly to the participating organization. CareFirst also recommended that only the authentication logs pertaining to the receiving participating organization should be made available and reviewed by the participating organization.

Staff action – Change made: Staff agrees with the requested changes and included language within Section .06F(3).

- CareFirst recommended that a participating organization should be provided notice when an HIE has reason to believe that a breach or violation has occurred as detailed in Section .07C(2)(a), particularly since the HIE is required to provide notice to each person whom the investigation indicated may have committed a breach or violation.

  Staff action – Change made: Staff agrees that the regulations should require the HIE to provide notice to the participating organization and added language to Section .07C(2)a.

- Kaiser noted that a notification of breach to the person who notified the HIE of the potential breach or violation, as detailed in Section .08A(1)(a), could potentially reveal PHI and that the regulations should clarify that the notice should be provided in accordance with applicable State and federal laws. Kaiser also noted that a substitute form of notice to a patient whose information was breached, where there is insufficient or out-of-date contact information, as detailed in Section .08C(3), could also reveal PHI.

  Staff action – Change made: Staff agrees that such notices should only be provided to the extent permitted by HIPAA and other federal and State privacy laws. Language was included within Sections .08A(1)(a) and C(3).

- FUSE Health Strategies suggested that a notice of breach should be provided not just to an "individual," but to a "person" in cases where the entity providing the notices has knowledge that another "person" is acting as the health care consumer for the patient. FUSE Health Strategies noted that in some instances the State or a legal firm or another entity is authorized to consent as a person in interest and "person" is a more inclusive term.

  Staff action – Change made: Staff agrees with the requested changes and included language within Section .02 B. (33)(b) and(e)(ii) and Section .08 C(1).

- FUSE Health Strategies recommended that "reasonable timeframe but no longer than 60 days," that is detailed in Section .08C(4) for a breach notification to a health care consumer should be changed to 3-to-5 days for notification. FUSE Health Strategies

also recommended that MHCC contact information be provided within the breach notice to a health care consumer provided in Section .08C(5)(f).

Staff action – No change: Staff believes that the timeframe specified in the regulations will enable users of the data to complete a thorough investigation concerning potential breaches

- JHHS noted that notification of violation of federal or State privacy or security law to the appropriate authorities by the participating organization and the HIE should be provided to the appropriate authorities to which reporting such violation is required by applicable law.

Staff action – Change made: Staff believes that the requested change is what the originally drafted language intended and included clarifying language within Section .08D(1)(a).

- The OAG-CPD recommended that a participating organization and HIE provide notice to the health occupation boards in the event of a breach or violation by a health care provider. Additionally, the OAG-CPD recommended that public notice be provided if there is a large breach of more than 50 patients, including a posting on the HIE's or participating organization's website or via a major print or broadcast media.

Staff action – No change: Staff believes that the current requirements around noticiation to appropriate authorities are sufficient. The regulations, as detailed in Section .08D, require that participating organization and HIE provide notice to federal and State authorities to which reporting such violation is required by law, and to MHCC. Additionally, MHCC is required to forward to the OAG-CPD notification of a breach under this regulation. Regarding public notice, staff believes that the current requirements around an audit, as detailed in Section .06E(3), are sufficient. An HIE is required to post on the home page of its website a summary report of the audit, if a breach or violation of the proposed chapter is found, or if the health information of more than 10 patients was improperly used, accessed, or disclosed.

- The MHA suggested that future regulations address required action to be taken by an HIE when it no longer operates in Maryland.

Staff Action – Change made: Staff agrees and added proposed language, as detailed in Section .09A(1)(d), to require HIEs to have provisions for reasonable notice to participating organizations and the Commission if the HIE ceases to operate in Maryland.

- ACLU-MD noted that health consumers are provided notice in cases of a breach of their information, as detailed in Section .07, and recommended that health care

consumers be provided with similar notice when the Commission takes an enforcement action against a person where there may have been a violation of this chapter involving that patient, as detailed in Section .09C(2).

Staff action – No change: Staff believes that the regulations are in alignment with similar enforcement activities.

- FUSE Health Strategies recommended that the notice to the person in violation should be provided via certified mail, and not just on the website, as detailed in Section .09C(2).

Staff action – No change: Staff notes that a definition of "notice" was added to the regulation.

Miscellaneous

- The MHAMD and Koss on Care stated that the definition of a health care consumer detailed in Section .02B(14), which includes the patient and a "person in interest" is unclear

Staff Action – No Change: Staff believes that in certain cases the regulation intends to address requirements related to a patient's information, and in cases where a notice is to be provided, for example, that notice may be provided to the patient or a person in interest that may be acting on behalf of the patient. The term health care consumer allows for both to apply in certain instances of the regulation, without the need to specify both a patient and a person in interest in those instances.

- Kaiser recommended that the regulations specify who is responsible for maintaining the Master Patient Index (MPI), as defined in Section .02B(22).

Staff Action – No Change: Staff believes that the regulations do not need to specify who is responsible for the MPI as this function is typically part of the HIE or its contractors; therefore, certain uses of PHI including those in the MPI, would apply.

- Kaiser suggested that an attorney should not be included as a "person in interest" within the definition in Section .02B(33).

Staff Action – Change made: Staff agrees that an attorney, generally, should not be included as a "person in interest" and removed this language and removed this language from Section .02B(33). However, remaining language in the definition does identify a medical power of attorney as a person in interest.

- Coventry noted that, depending on when the regulations become effective, the requirements may be difficult to implement given current requirement placed on Coventry around the Health Insurance Exchange.

  Staff action – No change: Staff believes that the regulations are likely to become effective in late Winter or early Spring 2014 and that the requirements should not be too onerous to implement in that timeframe.

- The OAG-CPD requested that a bond always be required, and not just at the discretion of MHCC, as detailed in Section .09A(2).

  Staff action – No change: Staff believes that requiring a bond in all instances would be unduly and unnecessarily burdensome

Notes of Support

- The MHA noted the significant improvements made to the regulation language, particularly around patient consent and sensitive health information. The MHA also mentioned that it is looking forward to continuing to work with MHCC to address requirements around certain secondary used not currently detailed in the regulations.

- CRISP stated that it believed that draft regulations have significantly improved during the comment process "as a result of the MHCC's ongoing outreach to members of the health care community in Maryland and the responsiveness of the MHCC to the input it received."