



Public Comments in Response to Proposed Amendments: COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information*

A Notice of Proposed Action to COMAR 10.25.18 was printed in the December 2, 2024 issue of the Maryland Register. The proposed amendments support the implementation of Chapter 798 (House Bill 1375), *Health Information Exchanges - Electronic Health Information - Sharing and Disclosure*, 2021; Chapter 791 (Senate Bill 748) and Chapter 790 (House Bill 1022), *Public Health – State Designated Exchange – Clinical Information*, 2021; and Chapter 296 (House Bill 1127), *Public Health – State Designated Exchange – Health Data Utility*, 2022.

Comment Period: December 2nd 2024 through January 2nd 2025

Table of Contents

1. Chesapeake Regional Information System for our Patients (CRISP)	3
2. HIMSS Electronic Health Record Association (EHRA)	10
3. Kaiser Permanente	15
4. Medical Information Technology Inc. (MEDITECH)	19
5. Oracle Cerner.....	22



January 2, 2025

Nikki Majewski

Maryland Health Care Commission

Submitted via email to mhcc_regs.comment@maryland.gov

RE: MHCC Seeks Public Comments on Draft Amendments to COMAR 10.25.07 and COMAR 10.25.18

Dear Ms. Majewski:

The Chesapeake Regional Information System for our Patients (“CRISP”), the state designated health information exchange (“HIE”) and health data utility (“HDU”) for Maryland, appreciates the opportunity to comment on the draft amendments to COMAR 10.25.07 and COMAR 10.25.18 (the “Draft Regulations”). CRISP connects to over 75 percent of clinicians in Maryland and is a “best-in-class” HIE and HDU. As such, we have significant experience working with and across interested parties to normalize data and present information based on the need of that party while upholding the privacy of patients. We are grateful for these groundbreaking regulations, which will continue to push forward not only the state of Maryland, but also the entire country.

COMAR 10.25.18.03(D) – Consent Management Application

The proposals in COMAR 10.25.18.03(D) seek to implement the country’s first “one-stop shop” to allow a patient to opt-out of data sharing across HIEs, which include electronic health records in Maryland. Without these regulations, patients may opt-out at one location, thinking they have opted-out of all data exchange within the state. CRISP has experienced many conversations with patients who are devastated to learn that their sensitive data is still being shared and that they must opt-out at every HIE, a daunting task for a patient, if it is even possible. We are grateful for these proposals and believe they will greatly reduce patient burden, while also increasing their choices and honoring their preferences in data sharing. Below, we share our detailed comments on specific proposals in this section.

Proposal: (1)(b) The State-designated HIE shall implement a consent management application that . . . allows a person in interest to view the interested patient’s opt-out status.

Comment: CRISP does not currently possess the technical ability to verify identity through a portal or other electronic system. Although we have explored options for doing so, the identity management required for the security we uphold would likely be cost prohibitive without additional funding. Therefore, CRISP relies on point-of-care verification and persons in interest providing copies of required documentation to CRISP; for each, the process is manual. We are interpreting these proposed regulations to continue to allow such manual identity verification, with the viewable opt-out status to be provided via email or other method selected by the person in interest. If this is not MHCC’s intention, we would request additional lead time and funding to create such a patient portal with the appropriate identity verification.

Proposal: (1)(c) The State-designated HIE shall implement a consent management application that . . . informs the person in interest of the types of electronic health information that may be shared or disclosed in accordance with §A(2)(a) of this regulation notwithstanding the choice to opt out.

Comment: Although CRISP can inform persons in interest of the types of electronic health information that may be shared by CRISP, we cannot represent the type of information that may be shared by other HIEs within the state of Maryland. Therefore, we suggest that this section be changed to state “ . . . types of electronic health information that may be shared or disclosed by *the designated HIE* in accordance with §A(2)(a) of this regulation notwithstanding the choice to opt out.” If this language is not included, CRISP could share with persons in interest the potential or likely types of data shared, but it would not be conclusive and could be misleading. Therefore, we believe this change will more accurately reflect and explain to patients the exchange of their data and consequences of their opt-out.

Proposal: (2) Within 6 months of the effective date of this regulation, the State-designated HIE shall make the consent management application it develops available to registered HIEs.

Comment: Within the suite of regulations proposed by MHCC, much is required of CRISP in the next 18 months. To meet all deadlines appropriately and prioritize each concurrently, we request that MHCC finalize this proposal to allow twelve (12) months from the date of publication. We believe this timeline will allow more fulsome pilots with other HIEs and time for us to learn from and implement changes based on those pilots. This additional lead time will lead to a smoother, overall roll-out after those 12 months.

Proposal: (3) The State-designated HIE shall implement the consent management application with a secure electronic interface that supports standardized interoperability between various recipient HIE systems.

Comment: CRISP is interpreting this proposal such that “standardized” does not necessarily mean “standards” as the health IT community would interpret standards, such as Data Segmentation for Privacy (DS4P). Rather, CRISP is interpreting any number of solutions, such as application program interfaces and secure file transfers that could convey the necessary information in a standardized way. We believe this interpretation brings the necessary flexibility to Maryland’s cutting-edge requirements, which will likely require agile approaches based on differing needs of Maryland’s interested parties. CRISP, as always, strives to use and implement health IT standards, and will do so within this effort, and continues to believe flexibility in data exchange is critical to Maryland’s success.

Proposal: (4)(b)(i) An HIE shall . . . Establish bi-directional connectivity with the consent management application within 18 months of receiving notification from the State-designated HIE that the application is operational.

Comment: CRISP assumes the other HIEs in the state will participate in pilots that we will be running as we stand-up the consent management application functionality. If that is the case, we believe that a twelve (12) month timeline will suffice for bi-directional connectivity. Based on our conversations with patients and with our Consumer Advisory Council, we believe that patients

assume when opting-out with CRISP, they opt-out with all other HIEs. Thus, we request MHCC finalize a 12-month timeline for bi-directional connectivity to make that assumption a reality for patients.

Proposal: (8) The State-designated HIE shall promptly notify the Commission and all HIEs any time the consumer management application is not operational and when services are resumed.

Comment: CRISP considers “not operational” to be a downtime of fifteen (15) minutes or more. If a functionality within our system becomes not operational, we follow our standard processes by sending out communication and making a banner available in our portal and website. We would interpret this proposal to allow for our standard procedures, as stated above.

Proposal: (9)(b) An HIE is not required to comply with §D(4)(b) of this regulation when . . . The consent management application is not operational.

Comment: Note that, if the consent management application is not operational, depending on the mode of bi-directional exchange, the data may need to be re-exchanged with CRISP. CRISP would work with any affected HIEs during a time the consent management application is not operational to ensure opt-out statuses conveyed during that time are received. MHCC may wish to require HIEs to ensure that opt-out statuses are re-conveyed if necessary if the consent management application becomes non-operational.

COMAR 10.25.18.13 Non-Controlled Prescription Drug Dispenser Reporting

CRISP has appreciated the collaborative process in creating the Noncontrolled Prescription Drugs Dispenser Data Submission Manual. Thus, our comments in this section are limited. We are grateful for all the interested parties that were willing to engage beforehand, and we hope to have similar engagement with the consent management application and Electronic Health Network Transactions. Even so, we believe there are a limited number of places these regulations could be improved, which we discuss below.

Proposal: (E)(1)(d) The State-designated HIE shall . . . Retain noncontrolled prescription drug information collected pursuant to this section for at least 5 years from the date of receipt.

Comment: Under COMAR 10.25.18.03, a “health care consumer has the . . . right to opt out of an HIE.” In the past, CRISP has interpreted this section to require us to delete or make un-useable all data for an opted-out consumer except for the areas discussed in subsection (2)(a) of the same section. We request that MHCC clarify whether this proposal is an exception to COMAR 10.25.18.03 or HIEs should not retain noncontrolled prescription drug information collected if a patient has opted-out. We believe this clarification is necessary to ensure both HIEs and consumers understand the implications of opting out.

Proposal: (E)(1)(4) The State-designated HIE shall make patient-specific prescription information submitted by dispensers under this section available for purposes allowed under applicable law.

Comment: In subsection (F)(1) of this section, dispensers are required to report on and after September 1, 2025. CRISP anticipates that there may be a period of time after collection that will require data normalization and testing in our system before it is fully available for display for those allowed to view it under applicable law. Therefore, we request that we receive an additional three (3) months after September 1, 2025 for this testing before we are required to display such data. Specifically, we request MHCC change this text to read “Beginning January 1, 2026, the state-designated HIE shall make patient-specific prescription information submitted by dispensers under this section available for purposes allowed under applicable law.”

Proposal: (E)(5) Upon written request for public health purposes, the State-designated HIE shall provide data collected under this regulation within 5 days to the Maryland Department of Health, local health departments, the Commission, or the Health Services Cost Review Commission.

Comment: Along with COMAR, CRISP is subject to other Maryland and federal law and regulations with which it must comply. CRISP can only provide data if allowed by such laws. To ensure that those reading the regulations are aware of such limitations, we recommend modifying this section to read, “Upon written request for public health purposes *and as allowed by applicable law . . .*” As MHCC knows, this change is not necessary; CRISP will abide by all laws. However, in our experience, we have found that ensuring all interested parties are aware of such limitations not only sets expectations, but also provides comfort to consumers engaged with such regulations.

COMAR 10.25.18.14 Operation of the State-designated HIE as a Health Data Utility

CRISP has been honored to serve as not only the state-designated HIE, but also the state-designated HDU for Maryland for the last several years. We are leading the nation in what is possible in reuseable data exchange with robust governance. We believe the proposals in this section are intended to codify the work and processes CRISP already has in place, memorializing core functions of an HDU. Our comments reflect this understanding and also make minor suggestions for clarification.

Proposal: (C)(2) The State-designated HIE may not redisclose financial information in electronic health care transactions it receives in accordance with COMAR 10.25.07.09 to any person other than the Commission.

Comment: Based on our experience, what is considered “financial information” varies greatly based on an individual’s or company’s concerns. We are interpreting “financial information” to be the “billed amount” and “allowed amount.” If we are correct in this interpretation, we request that MHCC clarify “financial information” accordingly by either adding a definition of the term or explicitly stating what it is intended to mean in this section. We believe such clarification will ensure all interested parties are on the same page when designing solutions and collaborating on COMAR 10.25.07.09.

Proposal: (C)(4)(a) The State-designated HIE shall (a) Develop a process in which requests for data are submitted and data are shared, and post this information on its website; and (b) Provide a written explanation for a denial of a request which shall include an appeal process.

Comment: Currently, CRISP accepts all requests for data and documents all outcomes for these requests when an individual contacts us through phone, email, or other means as stated on our

website. After first-line requests and answers are generated, requestors can speak with the CRISP Privacy Officer, who then further documents the results of these requests. We are interpreting this proposal to continue to allow our current process.

Proposal: (E) (1) The State-designated HIE shall establish a Consumer Advisory Council in accordance with Health-General, § 19-145, Annotated Code of Maryland. (2) The State-designated HIE shall: (a) Appoint two consumer representatives identified by the Commission who have significant experience in public health and patient privacy as council members; (b) Post advance notice of council meetings on its website, including an expected agenda; and (c) Require the Consumer Advisory Council to comply with the requirements of the Maryland Open Meetings Act as if it were a public body.

Comment: For two (2) years, CRISP has engaged our Consumer Advisory Council. This body has repeatedly requested that CRISP facilitate closed, confidential meetings to discuss concerns the members consider sensitive. Section 3–305 of the Maryland Open Meetings Act allows closed meetings if certain exceptions apply, including to “protect the privacy or reputation of an individual with respect to a matter that is not related to public business.” Therefore, we believe that most of these meetings can still be conducted privately, as requested by the Consumer Advisory Council. If our understanding is not correct, we request an exception in this section for confidential matters as determined by the Consumer Advisory Council. Specifically, we request that (c) be modified to read, “*except when the Consumer Advisory Council requests confidential meetings, as documented in writing, require the Consumer Advisory Council to comply with the requirements of the Maryland Open Meetings Act as if it were a public body.*”

COMAR 10.25.07.09 Electronic Health Network Transaction Submission

Electronic Health Networks provide a wealth of data that fills information gaps and are yet untapped in the state of Maryland. We are excited by these proposals and what they can bring to users of CRISP as they benefit the larger state. Below, we provide suggestions to ensure that this data can truly fill such gaps and meet the promise of the original legislation.

Proposal: (A) An MHCC-certified EHN shall submit electronic health care transactions information in accordance with this regulation to the State-designated HIE for public health and clinical purposes to facilitate: (1) A State health improvement program; (2) Mitigation of a public health emergency; or (3) Improvement of patient safety.

Comment: We are grateful for these regulations and believe that sharing of this data will greatly fill information gaps in health and healthcare, helping both consumers and providers alike. However, based on this proposal, CRISP believes MHCC is overly limiting the uses of this information. For example, “treatment” is not a blanket permitted purpose in these proposed regulations although it is under federal law; thus, the uses for providers may be limited if this proposal is finalized as is. Furthermore, the impending AHEAD model may not be able to use the information to inform its goals, including quality care and reduced costs. Perhaps most troubling, while this regulation states the data could be used to “mitigate” a public health emergency, it is not clear that it could be used to proactively prevent a public health emergency; that is, as written, the data likely could only be used once a public health emergency has been declared, when one of the goals of public health is to keep such emergencies from occurring at all.

Therefore, we request that MHCC modify this section to state, “An MHCC-certified EHN shall submit electronic health care transactions information in accordance with this regulation to the State-designated HIE for *any purpose allowed by applicable law.*”

Proposal: (I) The State-designated HIE shall publish the Electronic Health Care Transactions Technical Submission Guidance within six months of the final effective date of this regulation.

Comment: As MHCC knows, CRISP has actively and persistently attempted to engage Electronic Health Networks in pilot projects to help both us and them understand how to comply with potential regulations. Despite these attempts, we have not been able to launch a pilot. In addition, this type of data exchange is first in the nation, without a “playbook.” Therefore, to both create and publish the Electronic Health Care Transactions Technical Submission Guidance, we believe we would need *at minimum* twelve (12) months. This timeline is especially necessary given the competing priorities of the consent management application and the collection of non-controlled prescription drugs. With this additional time, we believe we can adequately complete these concurrent regulatory requirements, continuing our best-in-class leadership throughout the country.



CRISP highly values its relationship with the Commission and is honored to serve as the state designated HIE and HDU for Maryland. As we engage throughout the country, there is no doubt that Maryland is best-in-class and is leading the way with other states. We look forward to continuing to leadership role, as we work together to implement these ground-breaking regulations.

Best,

Craig R. Behm
CEO and President, CRISP

January 15, 2025

David Sharp, Director
Center for Health Information Technology and Innovative Care Delivery
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

Re: Proposed Revisions to 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Director Sharp,

On behalf of the 29 member companies of the HIMSS Electronic Health Record (EHR) Association, we appreciate the opportunity to provide feedback and recommendations on the proposed revisions to *10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information*. As the trade association of EHR developers serving healthcare providers and organizations in Maryland and across the United States, we work together to accelerate health information and technology adoption, advance interoperability, and improve the quality and efficiency of care.

As shared in our [May 2024 comments](#) on the informal draft amendments to COMAR 10.25.18, integration of a Consent Management Application and HIEs as proposed in these revisions will have a significant impact on both EHR developers, in the context in which Maryland has defined EHR developers as Health Information Exchanges (HIEs), and the providers and health systems that license, configure, and use those EHRs. As such, we appreciate the opportunity to share our concerns about the proposed changes, including our concerns about the lack of clarity on how or why a developer of Certified Health IT would be required to interact directly with a Consent Management Application.


We also recommend that a timeline of 30-36 months be established for healthcare providers to broadly adopt the Consent Management Application from the point at which this feature is made operational by the state and CRISP. This timeline also better supports the application's ability to coordinate with HIEs and healthcare providers to ensure their ability to support onboarding activities statewide.

These and other concerns and recommendations are explained in greater detail below. We welcome the opportunity to continue collaborating with MHCC on these and related issues.

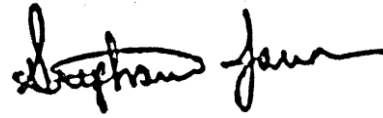
AdvancedMD	Elekta	Greenway Health	NetSMART	Sevocity
Altera Digital Health	EndoSof	Harris Healthcare	Nextech	STI Computer Services
Athenahealth	Experity	MatrixCare	NextGen Healthcare	TruBridge
BestNotes	Epic	MEDHOST	Office Practicum	Varian – A Siemens Healthineers Company
CureMD	Flatiron Health	MEDITECH, Inc.	PointClickCare	Veradigm
eClinicalWorks	Foothold Technology	Modernizing Medicine		

Thank you for your consideration.

Sincerely,



Leigh Burchell
Chair, EHR Association
Altera Digital Health



Stephanie Jamison
Vice Chair, EHR Association
Greenway Health

HIMSS EHR Association Executive Committee



David J. Bucciferro
Foothold Technology



Danielle Friend
Epic



Michelle Knighton
NextGen Healthcare



Ida Mantashi
Modernizing Medicine



Shari Medina, MD
Harris Healthcare

Established in 2004, the Electronic Health Record (EHR) Association is comprised of 29 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families. The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.

Electronic Health Record Association

Proposed Revisions to 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information – Feedback and Recommendations from the EHR Association

.01 Scope and Purpose

Applicability to Health IT Developers of Certified Health IT

While Maryland defines a Health IT Developer of Certified Health IT as an HIE, it is not a data holder and therefore cannot be required to deploy and/or interact with patient data. Health IT Developers of Certified Health IT typically do not have custody of Electronic Health Information and, as such, do not have any way to directly manage individuals' consent/authorization decisions. Rather, they provide software and services as business associates of the healthcare providers and others in the healthcare ecosystem who have full custody of such information. The role of a Health IT Developer of Certified Health IT should be to develop functionality that can be deployed and used by the healthcare providers and HIEs that directly interact with patients to interact with a Consent Management Application and process patients' consent/authorization decisions. Thus, at a fundamental level, it is unclear how or why a Health IT Developer of Certified Health IT would ever need the capability to interact with a Consent Management Application.

Requiring Health IT Developers (or others without direct patient access) to interact with a Consent Management Application could result in a scenario where Health IT Developers have inappropriate access to data within the Consent Management Application, despite having no direct relationship with patients. This would result in broader access than necessary to the consent decisions of Maryland patients, broadening the Consent Management Application's privacy and security risk profile. It would also create an additional burden on health IT developers without providing additional benefits to patients or healthcare providers.

MHCC should adopt an approach in regulation that recognizes the unique role of Health IT Developers of Certified Health IT within Maryland's HIE regulations. The final regulation should require that Health IT Developers of Certified Health IT incorporate functionality into the software used by healthcare providers that enables healthcare providers to interact with the Consent Management Application but clarify that the Health IT Developers themselves do not have responsibility for Consent Management.

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

Exception. Section D(4)(b) of this regulation does not apply to an HIE that solely exchanges electronic health information with other HIEs and does not have any health care providers as a participating organization.

We appreciate MHCC's recognition that different actors have different roles within the health data exchange ecosystem. This exception appears to be intended to exempt actors that play a role merely as a facilitator of exchange from requirements to interact with the Consent Management Application. We

support such an exception since these types of entities are not themselves responsible for deciding whether the exchange or disclosure of health information should take place.

It's important to recognize, however, that the entity first releasing the patient's record for exchange (e.g., the healthcare provider) should have the responsibility of reviewing whether the disclosure/exchange is consistent with the consent provided by the patient. The entity that legally holds the data should clearly have a different responsibility than an HIE that simply executes an exchange deemed appropriate by the healthcare provider. An HIE should only be required to connect with the Consent Management Application if it preserves copies of patient records and can also independently disclose those records through exchange processes.

Moreover, we are not aware of any HIEs (as traditionally defined) that play the role of facilitating/executing exchanges without also having healthcare providers as participating organizations. As a result, this proposed exception will not have its intended effect. We recommend that the exception instead state that the regulation does not apply to an HIE that does not maintain copies of patient records that it can independently choose to disclose through exchange processes.

Establish bi-directional connectivity with the consent management application within 18 months of receiving notification from the State-designated HIE that the application is operational;

Other jurisdictions that have finalized requirements to connect to similar Consent Management Applications have found significant complexity in projects aimed at enabling bi-directional exchange with healthcare providers using EHR software. Success requires the developer of the Consent Management Application to publish clear, well-tested specifications for connectivity. It also requires developers to have sufficient time to design, develop, and test updates to EHR software, as well as time for healthcare providers to implement new functionality, and also train their users.

Additionally, HL7 FAST is developing a set of Consent Management App-focused FHIR-based implementation guidance which will be critical to the successful and consistent use across all Health IT required to manage, share, and access patient data sharing consents. Building on industry standards and guidance will be critical to successfully scaling this within Maryland and other states where a patient may go for their care.

Thus, we recommend a timeline that allows 30-36 months for the broad adoption of this feature by healthcare providers from the point at which the Consent Management Application is operational. This will also better support the Consent Management Application's ability to coordinate with HIEs and Healthcare Providers and ensure the state-designated HIE has the staff bandwidth to support the onboarding activities of all healthcare providers and HIEs in the state.

Update the HIE's system with the most recent version of the consent management application data at least every 5 business days;

A patient's consent decision could change within a five-business day period, leaving the HIE's decision to exchange their data uninformed by the patient's current preferences. Moreover, it's important to reflect in this regulatory process the fact that patients might express different consent preferences specific to individual providers from which they receive care, informed by the exact care they received. Specifically, they may be uncomfortable with certain diagnoses being shared with clinicians in other care settings

who they deem - right or wrong - to be someone who doesn't need to know about another condition or diagnosis, but they could be comfortable with that information being shared with other providers they consider more relevant. The regulation should reflect that challenge.

Instead of requiring HIEs to ingest the consent decisions of every patient every five business days, the HIE should be required to check the Consent Management Application for updated preferences from the patient before each disclosure of the patient's data through an HIE. This approach ensures that the patient's most up-to-date preferences are respected and simultaneously reduces the burden of needing to process the Consent Management Application's data for all patients every five business days.

The regulations and Consent Management Application will also need to accommodate the ability to respect consent preferences that vary across healthcare providers. Finally, as noted above, the regulation should address the need to have greater real-time synchronization of what is effectively a federated environment.

An HIE shall place a link on its website directing a person in interest to the State-designated HIE's website to globally opt out or opt in to having a patient's electronic health information shared or disclosed by an HIE.

This requirement should only apply to HIEs that have direct relationships with patients (e.g., because the HIE stores/preserves copies of patient records that it can independently choose to disclose).



Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc
2101 East Jefferson Street
Rockville, Maryland 20852

January 2, 2025

Ben Steffen
Executive Director
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

RE: Proposed Regulations: 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Mr. Steffen:

Kaiser Permanente appreciates the opportunity to comment on the proposed regulations for 10.25.18. Kaiser Permanente is the largest private integrated health care delivery system in the United States, delivering health care to over 12 million members in eight states and the District of Columbia.¹ Kaiser Permanente of the Mid-Atlantic States, which operates in Maryland, provides and coordinates complete health care services for over 825,000 members. In Maryland, we deliver care to approximately 475,000 members.

The draft indicates that the cost is currently unknown but is anticipated to be minimal given existing HIE infrastructure. KP expects this is unlikely for the consent management requirements. Not only does the consent management application not yet exist, but neither does the intended integration with HIEs and their participating providers. Our comments on specific proposed provisions are as follows:

1. State-Designated Consent Management Application (CMA)

- (03 D (1)(b)) states that the CMA must support an individual's ability to view opt in/opt out status. We recommend that the regulations indicate whether there is a self-service requirement for individuals to view this information online. If so, it should indicate that the solution must have appropriate privacy and security controls in place to ensure individuals can only view their own (and proxy) opt-out/opt-in status.
- We recommend a slight amendment to (03 D (1)(c)): "(The CMA must) Inform the person in interest of the types of electronic health information that may be shared or disclosed in accordance with §A(2)(a) and §A2(b) of this regulation notwithstanding the choice to opt out." Section §A2(b) identifies educational requirements, which is necessary to include in the CMA so that individuals can make informed decisions about opting out.

¹ Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., the nation's largest not-for-profit health plan, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 39 hospitals and over 650 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

2. HIE Connection to the Consent Management Application (CMA)

- We recommend that the draft include CMA functionalities that are adaptable to varying HIE architectures and capable of bidirectional data flow, given the need for universal applicability across diverse HIE architectures (not reliant solely on APIs).
- We also recommend flexibility in updating consent statuses only during transaction activity rather than a fixed 5-business-day cycle to optimize efficiency. Consider revising the requirement for consent status updates from a fixed 5-business-day cycle to real-time updates before patient information exchange. *However*, the solution must ensure that real-time consent checks with the CMA do not significantly slow down transaction times for clinical data exchange. (03 D (4)(b)(ii))
 - A challenge with the 5-day consent check is that provider organizations who participate in a federated HIE (like Kaiser Permanente with Epic’s Care Everywhere), will need to do a check every five days for the millions of patients within the entire EHR. Centralized HIEs would need to do it for all the patients within their EMPI as well. This would not be a cost-effective approach given that the vast majority of patients would not have any opt-out activity, and likely no HIE activity within that timeframe.
 - In KP’s previous comments on the informal draft regulations, we indicated that a real-time check would be problematic given performance concerns. Instead, we proposed a proactive push of the opt-out/in notification from the CMA to affected organizations based on patient rosters. A challenge with this approach, however, is that it would not provide notifications for historical patients that have records at KP and need to be opted out as well. As such, a better balance would be real-time checks to the CMA before patient information exchange.
- 03 D (7) states that an “HIE shall continue to manage local opt-outs locally.” It is unclear what is meant by a “local opt-out.” For example, consider defining it to mean when an individual chooses to opt out only from one specific HIE or provider (in a federated model) rather than defining it as opting out of all exchange within the state. In this scenario, the HIE/provider would opt the individual out of their system only and not send the update to the CMA.
 - Along these lines, we recommend that 03 D (4)(b)(iii) be updated to read that an HIE must, “[u]pdate the consent management application with any statewide, non-local opt-out or opt-in requests it has received from an HIE or directly from a person in interest within 5 business days.”

3. Feasibility of Technology Implementation Timelines

- The proposed 6-month turnaround for the state-designated HIE to develop the consent management application and 18-month timeline for bidirectional CMA connectivity (03

D(4)(b)) are ambitious given existing technological gaps. Current timelines for CMA connectivity and data segmentation are insufficient considering the technical and vendor challenges. We recommend extending compliance deadlines to 24-30 months post-finalization of technical standards to allow adequate testing, vendor readiness, and phased rollout.

4. Access, Use, or Disclosure of Sensitive Health Information (.04)

- We recommend that this section be updated to reflect that the Consent Management Application is not yet intended to manage consent for the release of sensitive information (e.g., SUD and reproductive health information). Individuals may desire that their non-sensitive information be shared through HIE, but not their sensitive information. The CMA is seemingly intended to do complete HIE opt outs at this point and, therefore, not functional to handle scenarios where patients only want to keep their sensitive information blocked. As such, the sensitive information authorizations are better equipped to be handled at the source systems for the time being.

5. Dispenser Reporting Adjustments

- We recommend establishing phased onboarding for dispensers, starting with larger entities and gradually incorporating smaller ones. We suggest scaling implementation with phased onboarding for dispensers and tiered reporting requirements based on capacity.
- KP is also opposed any potential future expansion of reporting requirements to include additional clinical data from providers into CRISP or to significantly broaden the scope of dispenser reporting to include more clinical information about non-controlled medications. Centralized data repositories are technically unnecessary, as federated systems can meet reporting and analytical needs securely and efficiently. A centralized model creates significant security risks by making repositories attractive targets for cyberattacks and breaches that threaten sensitive patient information. Furthermore, aggregated data carries the potential for exploitation, including commercial misuse, and introduces insurmountable conflicts of interest, including monetization and inappropriate data sharing. The inclusion of more clinical data, especially beyond the existing non-controlled medication scope, may lead to duplicative, outdated, and inconsistent records that compromise patient safety, provider liability, and the integrity of real-time care. While statewide health information exchange is critical, expanding reporting requirements without addressing these foundational risks undermines the principles of interoperability and confidentiality central to quality healthcare.

6. Public Health Data Utility and Consumer Advocacy

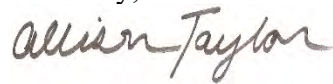
- We support the HDU's public health and equity objectives while safeguarding individual privacy. To that end, we recommend that consumer advocacy groups on the HDU Advisory Council are adequately represented to encourage transparent and productive engagement.

Other Recommendations

- **Vendor Engagement:** We recommend that MHCC consult with major EHR and HIE vendors before finalizing timelines and technical specifications.
- **Transparency and Collaboration:** We request that MHCC host regular forums for stakeholders, including providers, HIEs, and patient advocacy groups, to discuss implementation progress and address barriers.
- **Regulatory Flexibility:** We recommend that MHCC provide clear provisions for temporary waivers or extensions where significant technological barriers or public health emergencies exist.

Thank you for the opportunity to comment. Please feel free to contact Allison Taylor at Allison.W.Taylor@kp.org or (202) 924-7496 with questions.

Sincerely,



Allison Taylor
Director of Government Relations
Kaiser Foundation Health Plan of Mid-Atlantic States, Inc.

January 2, 2025

Nikki Majewski
Chief Health Information Technology
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

Dear Nikki Majewski:

Attention: COMAR 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information, Notice of Proposed Action [24-164-P]

On behalf of Medical Information Technology, Inc., I am pleased to offer comments on the *COMAR 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information Notice of Proposed Action [24-164-P]*.

MEDITECH empowers healthcare organizations around the globe to expand their vision of what's possible with Expanse, the intelligent EHR platform. Expanse answers the demands of an overburdened workforce: personalized workflows, interoperable systems, and innovative AI applications, all working together to drive better outcomes.

MEDITECH supports initiatives which seek to improve overall patient health and safety as well as the protection of private health information. However, MEDITECH has concerns with specific requirements related to the implementation of a consent management application.

Kindly find our feedback on the proposed amendments noted below.

Industry Challenges

MEDITECH has concerns with the integration of a newly implemented consent management application and Health Information Exchanges (HIEs), which include Electronic Health Records (EHR) vendors. Currently there is no complete, widely-adopted, centrally governed industry standard for this type of integration.

Further, MEDITECH, as well as the industry, is currently being challenged by other regulations (Federal - 42 CFR Part 2, Michigan - HB 5283 and New York - Part 300 of Title 10 NYCRR) proposing and finalizing legislation related to centralizing consent management. Differences in requirements makes it difficult to support a standard product for our users.

MEDITECH strongly urges Maryland's State-designated HIE to evaluate and consider the HL7 FAST Consent Management Implementation Guide (IG) currently in development and projected to be ready by summer. Using a standard consent architecture will allow for a scalable solution for multiple consent management use cases as well as allow for more precise validation testing.

Additionally, to ensure the technological feasibility of a workable integration across the industry, MEDITECH recommends development collaboration between the state-designated HIE and other HIEs. A collaboration will allow for all aspects of consent to be discussed and considered, leading to a more robust solution. MEDITECH strongly suggests the state-designated HIE lead a workgroup where design updates can be discussed and industry feedback can be provided during the development phase.

MEDITECH appreciates MHCC's consideration regarding the HIE's timeline of 18 months to "establish bi-directional connectivity". However, as this is a new development effort with no current industry standard, it is to be noted that this timeline should not be inclusive to a completed solution. Once the connectivity is established, extensive collaborative testing should occur between HIEs and the state-designated HIE to ensure accuracy and validity of the integration, as this can only be thoroughly tested when connectivity is established.

.03 1. Consent Management Application (4)(b)(iv)

MEDITECH has concerns with the following requirement under 'An HIE shall':

(iv) Withhold sharing or disclosure of the electronic health information of a patient to the extent the consent management application indicates that the patient has opted out of having electronic health information shared or disclosed by an HIE, except to the extent permitted by §A(2) of this regulation

MEDITECH kindly requests clarification regarding the definition of the phrase 'to the extent the consent management application indicates that the patient has opted out.'

Note: Should this mean a person in interest can dictate what data can and cannot be shared, MEDITECH recommends this is clearly defined as the data set that allows for this functionality will be very large and complex.

.04 1. Procedure for Disclosing or Re-disclosing of Part 2 Health Information

MEDITECH has concerns with the following requirements:

1. Procedure for Disclosing or Re-disclosing of Part 2 Health Information.

(1) An HIE shall be in compliance with Part 2.

(2) A [health care provider] participating organization that is a Part 2 program, as that term is defined by Part 2, shall identify itself as such and clearly indicate [on] with all of its patient records [that such records may only be disclosed by point-to-point transmission through an HIE, if appropriate patient consent or authorization has been obtained, or as otherwise permitted by these regulations.] any limits on use or disclosure required by Part 2.

[(2)](3)[A] An HIE or participating organization that receives Part 2 information may not re-disclose such information without appropriate patient consent or authorization [,] except as permitted by applicable federal and State laws and regulations.

MEDITECH would kindly request clarification within section (2) on what standard would need to be used by a participating Part 2 organization "to identify itself as such and clearly indicate with all of its patient records any limits on use or disclosure required by Part 2"?

Thank you for your time and consideration. We look forward to your responses in the final rule.

Sincerely,

Angela Hall, RN/bt

Angela Hall, RN
Program Manager, Healthcare Policy

Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

January 2, 2025

Dear Sir or Madam,

Oracle Health, a leading supplier of electronic health record, clinical and revenue cycle information systems appreciates the opportunity to submit comments on provisions of COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses and COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information. We offer comments on the following provisions outlined below.

Oracle Health hopes these comments will be of value to the Maryland Health Care Commission (MHCC) in considering possible updates to COMAR 10.25.07 and COMAR 10.25.18. We are happy to help clarify any of the comments should MHCC wish to pursue any such conversations with us during the period of comment review.

Sincerely,



Mike Hourigan
Sr. Director, Product Regulatory Strategy
Oracle Health Corporation

As a general consideration Oracle continues to raise concerns with the conflation of health IT being considered Electronic Health Networks (EHN) and Health Information Exchanges (HIE). In this context, there are widely different purposes, functions, and use of Electronic Health Records and Revenue Cycle Management systems supporting providers. HIE's enable data sharing across providers and other entities at a geographic (local, state, national) level, and Electronic Claims Clearinghouses as a specific intermediary network. Such conflation creates ambiguities in which health IT which is only responsible for certain capabilities, must be capable of everything. We suggest role-based definitions of functional and technical capabilities that are incorporated into ASTP/ONCs certification program provide a more practical and scalable approach to address the complexities of the health IT eco system at a state and national level.

10.25.07 Certification of Electronic Health Networks (EHN) and Medical Care Electronic Claims Clearinghouses. Reporting of Electronic Healthcare Transactions for Certified EHN or Clearinghouse

Electronic Health Network/Clearinghouse will submit electronic health care transactions originating in Maryland to the State Designated HIE

- Some of these transactions are single, “real-time” transactions and some are batch files. Does the EHN/Clearinghouse submit a data feed of real-time 270s/271s, or is it a batch up submitted on some sort of schedule? Clarification is needed as development will be necessary for this.
- Some trading partner contracts with payers restrict sharing of the data. See [Medicare transaction system \(HETS\) trading partner agreement \(TPA\)](#) as an example. Each payer including Medicare or private payer, may restrict the storing and sharing of the 271 responses as they consider that data proprietary. This may impact the allowance of transaction data sharing.
- All clearinghouses that transact with payers likely use intermediaries or other clearinghouses to route transactions to payers. Requirements should be clear and acknowledge who is required to submit electronic health care transactions. Is it the primary/contracted clearinghouse that is a registered EHN in Maryland only? We suggest that more specific role-based attribution of these capabilities and responsibilities would enable the relevant health IT to provide such capabilities.

EHN shall begin submitting electronic health care transactions information based on the most recent version of the Electronic Health Care Transactions Technical Submission Guidance within 12 months following the initial publication of the Technical Submission Guidance.

- Considering the development and deployment requirements to enable the proposed capabilities, we suggest that an EHN/Clearinghouse would need more than 12 months post publication of the technical submission guidance to develop and be able to submit electronic health care transactions to the state designated HIE, not considering the roll-out and deployment to all clients impacted. We recommend that 18 months is more feasible to develop and deploy the required solution.

Submit electronic health care transactions originating in Maryland to the State Designated HIE for public health and other clinical purposes.

- Clarification is needed on what transactions fall under this requirement. Specifically, does this mean all 270/271 transactions from any Maryland providers to any payer must be submitted by the appropriate EHN/Clearinghouse to the state designated HIE? Or do only 270/271 transactions from any Maryland provider to just Maryland payers (MD Medicaid, Blue, etc) need to be submitted by the appropriate EHN/Clearinghouse to the state designated HIE? We note that transactions originating in Maryland, may be subject to trading partner agreements as identified above.

10.25.18 Health Information Exchanges (HIE): Privacy and Security of Protected Health Information, Consent Management Application

Requirements for an HIE

“Update the consent management application with any opt-out or opt-in requests it has received from an HIE or directly from a person in interest within 5 business days.”

We request further clarification in the following areas:

- Does this require an HIE to use a CRISP app locally to manage opt in/out, or that the providers’ health IT can use CRISP provided APIs to maintain the relevant data?
- Oracle recommends, all communications with the central CRISP consent repository should be API based (with a clear migration path to FHIR-based APIs).

“Withhold sharing or disclosure of the electronic health information of a patient to the extent the consent management application indicates that the patient has opted out of having electronic health information shared or disclosed by an HIE”

- We note that the scope of an opt-out by the patient is effectively retroactive, i.e., when the patient opts out, no information (past, current, future) can be shared from that point forward by any health IT holding that patient’s information. Does that opt-out apply only to exchange within Maryland, or to any provider whether communicating directly or via a local, state or national network to the health IT holding the data? Conversely, when a patient is opted in with CRISP, can they opt out from national network exchange in particular, which could result in not sharing their data with other Maryland providers when data flows through the national network? Would a patient be required to manage opt in status with CRISP for national network sharing? And lastly, as other consent management tools emerge for the patient to manage all their consents across their providers and other data holders, what is the precedence relationship between the CRISP consent manager and the patient’s consent manager?

Considering the need for patient centric consent management tools that are on the cusp of emerging that enable a more robust approach than a state focused consent management approach, we urge Maryland to carefully advance its requirements that will not preclude if not prohibit such patient centric approaches.

- Considering the ambiguity of the reference to HIE and EHNs, would a Clearinghouse have to exclude submitting transactions where the patient has opted out? We suggest clarification of conditions and transactions where the opt out applies.

“An HIE shall place a link on its website directing a person in interest to the State-designated HIE’s website to globally opt out or opt in to having a patient’s electronic health information shared or disclosed by an HIE.”

- Centralized state consent managers are not patient centric (e.g., one might end up with four to five state-based repositories considering the proximity of Maryland to health care providers in neighboring states where patients can seek their care, e.g, PA, NJ, MD, DE, NY, VA). The focus should be advancing a patient centric approach towards capturing and managing a patient’s consent directives, one that is not artificially bound by jurisdictions. This makes it more agnostic and focuses on the essence that an opt-in/out directive is used to share or not share, rather than introducing an additional location where consent directives would be maintained.

“HIE shall Electronically notify authorized users when a patient has restricted data sharing.”

- We note that this statement is very ambiguous. What is considered an authorized user and of which health IT can know that the patient has restricted data sharing, particularly as such notification may in fact already divulge to the user what data may be. What action is the authorized user supposed to take having that knowledge? We suggest that within a provider’s health IT, it manages which users can or cannot see certain patient data and when data is not shared externally. There should not be an indication that data is not shared as that would impact the patient’s intent to not share data. Thus, raising the question of what, if any, exceptions there are to still share some information. Such exceptions need to be very well defined.

“An HIE shall implement the consent management application in a manner that is consistent with this chapter, its existing policies and procedures regarding use and disclosure of PHI and other personal identifiable information, and its technological capabilities.”

- We note that per the [48](57) [“Opt-Out”] definition the patient may utilize a consent directive management app of their own choice. We appreciate and support that flexibility in light of our prior comments. Given that, we suggest that this statement should be clear that data holders (whether EHRs or state HIEs) shall implement “consent management”, not “the consent management application” and focus on API based interaction with the CRISP consent management tooling, thus maintaining flexibility on how this is implemented and how it should evolve over time as we go more granular, advance a true patient centric approach to consent management, and the need to manage the interaction with jurisdictional privacy rules.

“An HIE shall continue to manage local opt-outs locally.”

- In context to our prior comments, this requirement would drive a patient to have to maintain their consent directives with all the data holders that manage some or all of their data. Rather we suggest that the approach is not that prescriptive at this time and allows for

patient centric consent management tools to emerge where the patient maintains their consents in one place of their choice, allowing others to access that designated repository for the full and most up-to-date directives. We recognize this is not a reality today, however, with the advances being made, it is a viable approach that should not be precluded through regulatory requirements to the contrary. At the same time, the statement does recognize that consent management has a clear need for provider side health IT, particularly an EHR, to have certain capabilities that a network would, could, or should not provide.

- Maryland is carving out a role for CRISP and firmly believes that a centralized, state-based consent management capability is essential. Given the above-described need for patient centric approach and the variant requirements for the different health IT, including networks, to manage data sharing in accordance with the patient's consent directives, the capabilities are more relevant and critical on the provider or more generally, the data holder side. Effectively, the data holder needs to assess on every transaction (query response or push) in whatever form (not just HL7/IHE doc exchange, but HL7 v2, HL7 FHIR AND anything else including proprietary) whether it can share, even if the information does not go through an HIE. And from a patient perspective, as we get to more granular consent controls, only having centralized state based consent repositories are not the answer. We therefore urge a flexible, federated approach that allows for, but does not require a state-based capability in the middle as it will still not provide the patient centric capabilities that are essential to manage the complex data sharing requirements across a national health IT eco system.

Data the Consent Management Application/ Health Data Utility will contain:

- **Personal identifiers consisting of the full name, date of birth, mailing address, telephone number and other unique identifiers of the patient and person in interest, if not the patient**
- **Communication contact preferences and the relationship to the patient.**
- **The date the patient's consent preferences were last updated.**
- **The Health Data Utility will Transmit clinical information or electronic health care transactions to the Maryland Department of Health, the Commission, or the Health Services Cost Review Commission for public health purposes upon written request.**

We note that full name, date of birth, mailing address, and telephone number to be used to match patients, but also "other unique identifiers". Further definition is needed considering that full name, date of birth mailing address, and telephone number are not identifiers, rather demographic data used in in patient matching. A state-designated HIE should reasonably use the Medical Record Number (MRN) across its participants in a Master Patient Index (MPI) to link it all together in the absence of a unique identifier that is statewide or national and acceptable to identify a large number of patients. Enabling a real patient centric consent repository to access it for all of a patient's consent directives, there should be a unique "address" to the patient specific consent repository that can be shared, and in combination with an authorization component can enable data holders to access that repository and allows them to assert the most current, applicable directives. A clearinghouse may not have all the EHR identifiers as part of these transactions, i.e. MRN, etc., but should include at least one of the identifiers that can improve on patient matching.

What is the scope of “Transmit clinical information or electronic health care transactions to the Maryland Department of Health, the Commission, or the Health Services Cost Review Commission for public health purposes upon written request.” Why is that stated here as this should not yield a larger scope of data sharing than already authorized by Public Health and patient under these proposals. This seems to require more data to be shared.

Since the Change Healthcare breach, providers send inquiries to the clearinghouse around security. We request for specifics around CRISP security practices.