

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.

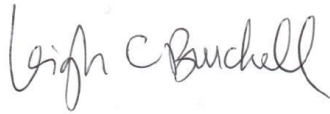
We also recommend that a timeline of 30-36 months be established for healthcare providers to broadly adopt the Consent Management Application from the point at which this feature is made operational by the state and CRISP. This timeline also better supports the application's ability to coordinate with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