MARYLAND Health Care Commission

Randolph S. Sergent, Esq., Chairman
Ben Steffen, Executive Director

Emergency Regulation: Informal Stakeholder Comments in Response to Draft Amendments

October 19, 2023

(1) COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information*

(2) COMAR 10.25.07, *Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses*

In support of Chapter 249 (House Bill 812), *Health – Reproductive Health Services – Protected Information and Insurance Requirements*

Comment Period: September 22nd through October 4th 2023

mhcc.maryland.gov

Toll Free: 1-877-245-1762
TTY Number: 1-800-735-2258
Fax: 410-358-1236

4160 Patterson Avenue
Baltimore, MD 21215

TABLE OF CONTENTS

athenahealth
80 Guest Street
Boston, MA 02135

Chapter 18.04 C: Developers of certified health IT will not be able to make the affirmation as written because it includes multiple components outside of their control and role. It is critical to rephrase the affirmation in (a) and (b) to better match the role of a developer of certified health IT, recognizing that the developer of the software cannot force healthcare provider organizations to install software updates or use particular features of the software:

- "(a) An affirmation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or (b) An implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."

Chapter 18.06 A(4): Consistent with these regulations, athenahealth shares MHCC's commitment to robust information security. However, we stress the need for agility and flexibility in these requirements. Serving as Business Associates as confirmed by HIPAA, developers of health IT already have thoughtful and robust security mechanisms in place such as NIST and DirectTrust. We urge MHCC to align requirements with HIPAA, as meeting additional state requirements would be overly burdensome with no value add to developers, patients, or providers.

Chapter 18.07 C: Developers of certified health IT conduct investigations of any breach or non-HIPAA violation that may have occurred. Under HIPAA, athenahealth is obligated to notify its customers of any unauthorized use or disclosure of PHI, including breaches of unsecured PHI. It would be unnecessarily burdensome to report each investigation to the Commission.

Chapter 18.10 A: athenahealth is supportive of and appreciates the flexibility MHCC offers by noting that an HIE shall not use or disclose a patient's sensitive health information for secondary use unless permitted by applicable federal or state laws and regulations.

As I noted we understand well the complexities of the political environment we find ourselves in and we strongly support your efforts to promote access to healthcare and protect patient privacy. However, those objectives must be achieved in a way that balances the need for appropriate information exchange within the healthcare system.

We welcome the opportunity to work together to ensure we achieve that balance and would love the chance to discuss these issues with you directly. Thank you again for your ongoing engagement and willingness to reach out to stakeholders, we appreciate the opportunity to support your important work. Please do not hesitate to contact me directly.

Thank you,

Joe Ganley
Vice President, Government and Regulatory Affairs

Cooperative Exchange
The National Clearinghouse Association

October 3, 2023

To the Maryland Health Care Commission

RE: Response to Title 10 Maryland Department of Health Subtitle 25 Maryland Health Care Commission Chapter 07 Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouse

The Cooperative Exchange (CE) is pleased to provide these informal comments to Title 10 MARYLAND DEPARTMENT OF HEALTH Subtitle 25 MARYLAND HEALTH CARE COMMISSION Chapter 07 Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouse. We understand the time limitations that the Commission is under to issue these rules, so we would be happy to discuss our comments with you via teleconference at your convenience.

As clearinghouses, the CE has been intensely interested in the requirements for submitting health care data to the Maryland State HIE. We have followed the development of rules and have previously sent you our comments on the implementation of these requirements (see attached). These new proposed rules raise additional areas of concern for us.

The proposed rules state

(1) By December 18, 2023, an MHCC-certified EHN shall submit to the Commission:

(a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX; or

(b) An implementation plan that includes:

(i) An affirmation that despite its best efforts, the MHCC-certified EHN lacks the technological capability to fully comply with Health-General Article, §4-302.5, Annotated Code of Maryland as of December 1, 2023, including a detailed explanation of the EHN's limitations;

(ii) A detailed description of the steps the MHCC-certified EHN is taking to ensure compliance with Health-General Article, §4-302.5, Annotated Code of Maryland by June 1, 2024;

The Cooperative Exchange (CE) is comprised of 23 of the leading clearinghouses in the US. The views expressed herein are a compilation of the views gathered from our member constituents and reflect the directional feedback of the majority of its collective members. CE has synthesized member feedback and the views, opinions, and positions should not be attributed to any single member and an individual member could disagree with all or certain views, opinions, and positions expressed by CE.

(iii) A timeline to implement Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX Aby June 1, 2024; and

(iv) A description of the extent legally protected health information and other health information will be restricted by the MHCC-certified EHN during the implementation of its plan.

(2)If a MHCC-certified EHN submits an implementation plan in accordance with §B(1), the EHN shall:

(a) Provide a status report to the Commission by April 1, 2024 detailing the progress the MHCC-certified EHN has made under its implementation plan; and

(b) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law.

The Cooperative Exchange has documented the following concerns with the proposed rule:

1) The scope of data to be protected is unclear and undefined at this time. The Secretary has not yet specified the procedure, diagnosis, medication and other related codes subject to restrictions of disclosure under §4-302.5(B) as required by §4-302.5(D). Furthermore, the CE previously submitted six areas of consideration to the MHCC in implementing the provisions of §4-302.3(h)(1) which requires "An electronic health network shall provide electronic health care transactions to the State–designated health information exchange for the following public health and clinical purposes: (i) A State health improvement program; (ii) Mitigation of a public health emergency; and (iii) Improvement of patient safety". The data to provide to the Health Information Exchanges (HIEs) and the manner in which it would be provided has also not been defined. These requirements would compel clearinghouses to disclose data to the seemingly outside the carve out provisions of §4-302.5(B) as required by §4-302.5(D). While clearinghouses excel at the technical requirements of filtering specified data sets within the scope of defined use cases, the lack of clarity proves prohibitive in setting a date for compliance as required by the proposed affirmation.

2) Clearinghouses are unable to decipher restrictions on the sharing of data at the patient level. As stated in our letter of February 25, 2021 to the State of Maryland General Assembly, "EHN trading partner relationships are typically administrative and contractual in nature with billing providers, vendors, and payers, vs. directly responding to requests for a single patient's electronic healthcare information (administrative or clinical). The patient is typically not in a contractual relationship with the EHN." Clearinghouses, while sharing a common business purpose of transporting transactions between authorized entities, have different business models which may not be suitable for these purposes.

   Transactions can be exchanged through clearinghouses without examining the contents. This makes decisions based on the meaning of the data challenging. Determining if legally protected health information is included in the transaction may not be possible as the data is exchanged by the clearinghouse.

The Cooperative Exchange (CE) is comprised of 23 of the leading clearinghouses in the US. The views expressed herein are a compilation of the views gathered from our member constituents and reflect the directional feedback of the majority of its collective members. CE has synthesized member feedback and the views, opinions, and positions should not be attributed to any single member and an individual member could disagree with all or certain views, opinions, and positions expressed by CE.

While most clearinghouses do validate the integrity of the transaction, its structure, and at times evaluate according to certain billing rules or 'edits', there is no mechanism or source of truth to validate that service actually happened as it was coded. The designated record holder is the provider and only they have the means to validate against the patient's chart.

3) Further, clearinghouse relationships are with the provider, not the patient. There is no mechanism to authenticate the identity of the patient reflected in the transactions. Unless the provider designated in each transaction, clearinghouses do not have the means to know if the patient or recipient gave authorization to release their legally protected health information. In performing the function of exchanging administrative transactions between providers and health plans, clearinghouses maintain that all transactions exchanged are related to claims processing. As Covered Entities and Business Associates, clearinghouses are already restricted under HIPAA for any disclosures outside of treatment, payment or healthcare operations. The Cooperative Exchange has made known our misgivings regarding the EHN disclosures made to the state in our prior correspondence which we have attached hereto for reference.

The CE appreciates the opportunity MHCC has provided to comment on such a complex undertaking. We believe that current information available in the law and proposed rule needs additional clarity and mutual cooperation to define the use cases and overcome operational and technical shortcomings to meet the goals of the Maryland legislature. **Due to the reasons specified above, clearinghouses should specifically be exempted from the requirements in the proposed rule** and any futures affirmations of preparedness for reasons set forth above and in our attached correspondence.

Sincerely,

Pam Grosze, Board Chair, The Cooperative Exchange,
Vice President, Product Manager Lead, PNC Healthcare

The Cooperative Exchange Background

The Cooperative Exchange is a nationally recognized association representing the healthcare clearinghouse industry in the United States. Our 23[1] clearinghouse member companies represent over 90% of the nation's clearinghouse organizations and process over 6 billion healthcare claims, reflecting over 2 trillion dollars in billed services annually. Our association members enable nationwide connectivity between over 1 million provider organizations, more than 7,000 payers, and 1,000 Health Information Technology (HIT) vendors. The Cooperative Exchange truly represents ***the U.S. healthcare***

The Cooperative Exchange (CE) is comprised of 23 of the leading clearinghouses in the US. The views expressed herein are a compilation of the views gathered from our member constituents and reflect the directional feedback of the majority of its collective members. CE has synthesized member feedback and the views, opinions, and positions should not be attributed to any single member and an individual member could disagree with all or certain views, opinions, and positions expressed by CE.

electronic data interstate highway system enabling connectivity across all lines of healthcare eCommerce in the United States.

The Cooperative Exchange member clearinghouses support both administrative and clinical industry interoperability by:

- Managing tens of thousands of entities and connection points
- Exchanging complex administrative and clinical data content in a secure manner
- Supporting both real-time and batch transaction standards
- Enabling interoperability by normalizing disparate data to industry standards
- Delivering flexible solutions to accommodate varying levels of stakeholder readiness (low tech to high tech)
- Providing strong representation and participation across all national healthcare standard and advocacy organizations with many of our members holding leadership positions

Therefore, we strongly advocate for standardization and administrative simplification within the healthcare industry.

The Cooperative Exchange (CE) is comprised of 23 of the leading clearinghouses in the US. The views expressed herein are a compilation of the views gathered from our member constituents and reflect the directional feedback of the majority of its collective members. CE has synthesized member feedback and the views, opinions, and positions should not be attributed to any single member and an individual member could disagree with all or certain views, opinions, and positions expressed by CE.

October 4, 2023

Ben Steffen
Executive Director
Maryland Health Care Commission
Submitted via email to mhcc_regs.comment@maryland.gov

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

Dear Executive Director Steffen:

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"). These amendments to COMAR stem from language in Chapter 249 (House Bill 812), *Health – Reproductive Health Services – Protected Information and Insurance Requirements* (the "Act"), adopted in 2023, on which CRISP provided testimony in both the House and Senate.

CRISP connects to over 75 percent of clinicians in Maryland. CRISP is committed to patient privacy and considers patient choice paramount. We allow patients to entirely opt-out of the HIE; we also provide patients with an auditing of every disclosure made through the HIE; in addition, we work with a Consumer Advisory Council on issues of privacy and request approval from our data governance committees before sharing data for new purposes. Thus, CRISP is committed to both the appropriate exchange of health data *and* the privacy and choice of Marylanders; as the state designated HIE and HDU, CRISP appreciates and navigates the technical issues required to put the Draft Regulations into effect as intended. Below, we provide comments on the Draft Regulations, and we encourage the Maryland Health Care Commission (the "Commission") to reach-out with any questions as we collaboratively work to balance the privacy and interoperability of health records.

COMAR 10.25.18.02 – Definitions

Proposal: (B)(40) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.

Comment: As we noted in our testimony,[1] the industry is not yet capable of what is called "segmenting data." Put simply, we can't take a health record and delete or stop the exchange of individual lines of data. This is a known issue because of our experience with the 42 CFR Part 2 regulations – those regulations require affirmative consent of a patient before certain substance use records are shared. Often, patients receive care in addition and separate from substance use in the same visit, but because technology cannot "segment" the substance use disorder data from the "other" data, the entire record is blocked. This result has been an issue for decades, and we know the consequences – patient records are stored in separate places and never exchanged – so these patients have siloed and incomplete data and, as a consequence, health care that has real and sometimes life-threatening effects on their health.

Due to these concerns, CRISP asked that the legislature to amend the bill to specify certain code sets that should be filtered and protected when going out-of-state. CRISP will be able to block specified codes, beginning with records with those codes and expanding to just the codes themselves. The successful implementation of the legislation relies on tying the definition of "legally protected health information" to specific diagnosis codes. Therefore, we ask the Commission to amend its proposal as follows to make clear that the protected information ties directly to the codes provided by the Sensitive Health Care Commission.

Suggested Proposal: *(B)(40) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b)* ***as specified by the Sensitive Health Care Commission established under*** *Health-General, §4-310, Annotated Code of Maryland****, as codified in*** *COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.*

COMAR 10.25.18.05 – Access, Use, or Disclosure of Protected Health Information

Proposal:
(C)(1) An HIE shall be in compliance with Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX.
(2) By December 18,2023, an HIE shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law; or (b) An implementation plan that includes:

(i) An affirmation that despite its best efforts, the HIE lacks the technological capability to fully comply with §C(1) of this regulation as of December 1, 2023, including a detailed explanation of the HIE's limitations; (ii) A detailed description of the steps the HIE is taking to ensure compliance with §C(1) of this regulation by June 1, 2024; (iii) A timeline to implement the requirements Health-General Article § 4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX by June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted through the HIE during the implementation of

[1] Committees - Media (maryland.gov).

its plan. (3) If an HIE submits an implementation plan in accordance with §C(2)(b), the HIE shall: (a) Notify all participating organizations by December 18, 2023 that the HIE is unable to comply with §C(1) with a written notice that describes the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan; (b) Provide a status report to the Commission by April 1, 2024 detailing the progress the HIE has made under its implementation plan; and (c) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law. (4) The Commission shall consider an HIE's implementation plan and reported progress when assessing penalties for a violation of this section.

Comment: We appreciate the intent of the Commission's proposal, which we believe to be requiring HIEs to either comply with the Act or explain their plan and when they will be complying with the Act. Based on our experience working with other HIEs to implement this law, however, we are concerned that some HIEs may submit an affirmation of compliance but are "complying" by entirely blocking a record. In addition, the Act specifies that patients should be able to consent to release such information. Therefore, we encourage the Commission to explicitly state that the affirmation include an explicit statement that the HIE can (1) block specific codes and convey the remainder of the record without blocking the entire record; and (2) allow a patient to consent to exchange of the protected data.

Suggested Proposal:

(C)(1) An HIE shall be in compliance with Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX.

(2) By December 18, 2023, an HIE shall submit to the Commission: (a) An affirmation that it possesses the technological capability to ***(i)*** *filter and restrict from disclosure legally protected health information to the extent required by law* ***and that it is parsing such codes and conveying all other information in the Health Record that is not prohibited by law to exchange; and (ii) allow patients to consent to the exchange of Legally Protected Health Information****; or (b) An implementation plan that includes:*

(i) An affirmation that despite its best efforts, the HIE lacks the technological capability to fully comply with §C(1) of this regulation as of December 1, 2023, including a detailed explanation of the HIE's limitations; (ii) A detailed description of the steps the HIE is taking to ensure compliance with §C(1) of this regulation by June 1, 2024; (iii) A timeline to implement the requirements Health-General Article § 4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX by June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan. (3) If an HIE submits an implementation plan in accordance with §C(2)(b), the HIE shall: (a) Notify all participating organizations by December 18, 2023 that the HIE is unable to comply with §C(1) with a written notice that describes the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan; (b) Provide a status report to the Commission by April 1, 2024 detailing the progress the HIE has made under its implementation plan; and (c) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law.

(4) The Commission shall consider an HIE's implementation plan and reported progress when assessing penalties for a violation of this section.

COMAR 10.25.18.06 – Auditing Requirements

Comment: The Commission makes several proposals under this section; however, these proposals do not seem to be connected to the Act and, therefore, are not in need of emergency regulations. Furthermore, it is our understanding that the Commission intends to release proposed regulations unrelated to the Act for notice and comment, as required by law. Those proposed regulations are much more comprehensive and some of the proposed changes therein may impact the proposals in this section, leading to a lack of full notice and consideration by the impacted constituents. Therefore, we request that the Commission decline to finalize any proposals in this section and, instead, allow them to be a part of the notice and comment process with the remainder of the proposed regulations not required by the Act.

COMAR 10.25.18.07 – Remedial Actions to be Taken by an HIE

Comment: The Commission makes several proposals under this section; however, these proposals do not seem to be connected to the Act and, therefore, are not in need of emergency regulations. Furthermore, it is our understanding that the Commission intends to release proposed regulations unrelated to the Act for notice and comment, as required by law. Those proposed regulations are much more comprehensive and some of the proposed changes therein may impact the proposals in this section, leading to a lack of full notice and consideration by the impacted constituents. Therefore, we request that the Commission decline to finalize any proposals in this section and, instead, allow them to be a part of the notice and comment process with the remainder of the proposed regulations not required by the Act.

CRISP highly values its relationship with the Commission and is honored to serve as the state designated HIE and HDU for Maryland. We look forward to implementing the most workable and practical solution that continues to protect the privacy of Marylanders.

Best,

Craig R. Behm
CEO and President, CRISP

October 4, 2023

BY EMAIL
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215
mhcc_regs.comment@maryland.gov

Re: Comments to Draft Emergency Amendments to COMAR 10.25.18 (the "Draft Regulation")

To Whom It May Concern,

Delaware Health Information Network ("DHIN") is a statutory instrumentality of the State of Delaware that operates as the State-approved provider of health information exchange services and the operator of the State of Delaware's Health Care Claims Database. In fulfilling those dual mandates, DHIN operates in Delaware and surrounding states, playing a critical role in the accurate and timely sharing of health data needed to improve care and ensure positive outcomes for patients. DHIN has engaged in myriad partnerships throughout the mid-Atlantic region, including a long-standing and successful relationship with the State of Maryland's State-sanctioned provider of health information exchange services, CRISP. While DHIN's primary sphere of operations is in Delaware, due to the fact that individuals in both Delaware and Maryland routinely cross our mutual border to obtain health care, in 2023 DHIN registered to do business as a health information exchange in Maryland.

DHIN agrees with the State of Maryland and the Maryland Health Care Commission that ensuring that patients and health care providers that are subject to a "substantial risk … that would result from disclosure" of sensitive information, including abortion care and directly related procedures, are appropriately protected is an important and laudable goal.[1] Equally important, however, is that any additional limitation on disclosure beyond what is already required by well-understood and long-standing legal protections does not unduly restrict the flow of important health information to those involved in the patient's care. Such a paradigm could inadvertently risk the health and well-being of the patient or potentially cause inadvertent damage to the provider or other permitted accessor. In light of the need to balance these priorities, DHIN appreciates the Health Care Commission's offer to review public commentary and submits the following comments to the Draft Regulation for consideration:

[1] *See* Md Code Ann., Health-General §4-302.5(d)(1) (requiring the Secretary to determine the appropriate data that should be subject to restrictions on disclosure "due to a substantial risk to patients or health care providers that would result from disclosure").

COMAR 10.25.18.02B(40): Overbroad Definition of "Legally Protected Health Information" and Lack of Compliance With Requirement to Identify Specific Code Sets

Health-General Article §4-302.5 (the "Enabling Act"), the statutory authority prompting the changes proposed by the Draft Regulations, makes clear that the limitation on disclosure prompted by that legislation should be targeted to information strictly necessary to prevent a substantial risk of damage to patients or health care providers. In so doing, the Enabling Act requires the Secretary to "determine for abortion care and sensitive health services the procedure, diagnosis, medication, and other related codes that are subject to the restrictions on disclosure under subsection (b) of this section ***due to a substantial risk to patients or health care providers that would result from disclosure.***"[2]

The Draft Regulations are not limited to data that presents a "substantial risk to patients or health care providers" and do not contain the code sets required by the Enabling Act. Instead, the Draft Regulations require HIEs and other affected entities to restrict access to *all* Maryland "abortion care" information, as well as "sensitive health services," which is defined by relevant Maryland law as "includ[ing] reproductive health services other than abortion care."[3] As currently designed, therefore, the Draft Regulations require HIEs to restrict access to *all reproductive health services information*, without any definitional qualifiers or specified code sets, and apparently without regard to whether disclosure of the data in question pursuant to the existing requirements with respect to the sharing of protected health information would cause a "substantial risk" to the patient or the provider of the reproductive health services.

This current state poses both legal and operational challenges to those who will be bound by the Draft Regulations. As an initial matter, the definition of "legally protected health information" is overbroad, as it requires HIEs to further restrict access to all "reproductive health services" without regard to whether compliance with the long-standing and well-established requirements of the Health Insurance Portability and Accountability Act and associated regulations ("HIPAA") and other relevant state law are sufficient to protect a patient's rights (as has been the case prior to the Enabling Act). In so doing, the Draft Regulations do not take into account the Enabling Legislation's requirement that any of these significant additional restrictions on the sharing of data be limited to circumstances where disclosure as permitted by HIPAA and relevant state law presents a "substantial risk" to the patient or health care provider.

A related concern is that the Draft Regulations do not include the specific codes that can be used by HIEs to identify legally protected health information, as required by the Enabling Act. Without further definitional clarification and these codes, HIEs end up in an untenable situation:

[2] Health-General §4-302.5(d)(1)
[3] Draft Amendment to COMAR 10.25.18.02B(40) (defining "legally protected health information"); Health-General §4-301(r).

they will have to determine for themselves what data the State of Maryland intends to include in its understanding of "abortion care" and "reproductive health services," and which data that falls into that category presents a "substantial risk" to the patient and provider if disclosed pursuant to existing laws and regulations. If the HIE underdesignates information, it risks substantial penalties from the State of Maryland. If it overdesignates, it risks running afoul of federal information blocking regulations, which require HIEs to send all relevant information to permitted requestors unless specifically prohibited by relevant law. Overdesignation also risks patient health, as it could prevent important information from being shared with parties permitted by HIPAA and associated regulations to access the data, including treatment providers, from having information at their fingertips that is material to their treatment choices.

In addition to the statutory compliance and patient safety issues, the lack of a well-defined and targeted set of codes associated with the restricted transmission of data will make the timing of compliance much more difficult. The limitation of specific code sets from the standard and well-accepted legal requirements with respect to data sharing is already a significant and additional burden on HIEs; asking those HIEs to develop their own code sets in the absence of specific guidance makes an already-difficult task significantly more onerous.

DHIN therefore respectfully requests that, prior to implementation of the Draft Regulations, and as required by the Enabling Legislation, the definition of "legally protected health information" in draft COMAR 10.25.18.02B(40) be narrowed to include only specific categories of data, identified by diagnostic or similar codes, the disclosure of which would create a "substantial risk to patients or health care providers."

Proposed Exception Process

Related to DHIN's concern about the current overbreadth of information subject to the Draft Regulations is the fact that there are other methods of protecting patients and providers from harmful disclosures of data that have been implemented by other states, including Delaware. Those methods provide alternative means to achieve the same laudable goal as that which went into the development of the Draft Regulations, and ensure that no "substantial risk" to patient or provider will be caused by disclosure.

By way of example, the State of Delaware has chosen to protect patients who receive care for reproductive services in the State by limiting the ability of third parties not authorized by HIPAA to access information from receiving that data through subpoena or other compulsory process. DHIN itself is a State instrumentality, and its enabling legislation has always made clear that "[h]ealth information and data held by DHIN is not subject to … subpoena by a court."[4] The State of Delaware has also taken steps to ensure that criminal or civil summonses directed to a

[4] 16 *Del. C.* § 10307(b).

provider or other organization in the State seeking data in support of a civil or criminal cause of action for engaging in medical procedures permitted in the State of Delaware – including abortion – will not be enforced.[5]

The upshot of these protections is that providing reproductive health or abortion data to an organization like DHIN, which is a State instrumentality in a state with significant legal protections for this data already in place, does not represent a "substantial risk to patients or health care providers" within the meaning of the Enabling Act.[6] DHIN therefore respectfully requests that the Health Care Commission modify the Draft Regulations, to provide an exemption to the increased disclosure limitations for state-chartered and state-sanctioned providers of health information exchange services that can provide proof to the Health Care Commission sufficient to satisfy the Health Care Commission that disclosure of abortion care and related information to the HIE will not "substantially risk" the patient or provider who provided those services in Maryland. Should the Health Care Commisssion be open to such a process, DHIN respectfully suggests that the exemption could be reviewable on an annual basis, in connection with the already-required annual registration by an HIE to do business in the State of Maryland, to account for a potential change in laws.

* * *

Thank you for the opportunity to provide commentary on what is an important and meaningful step in our shared efforts to protect patient confidentiality and permit healthcare and supporting service providers to access data that they need to continue improving patient outcomes.

Respectfully submitted,

/s/ Scott W. Perkins

Scott W. Perkins
General Counsel and Privacy Officer

[5] 10 *Del. C.* § 3928 (declaring laws that authorize a person to bring a civil action against a person who receives or provides abortion care as against the public policy of the State, and preventing the State from issuing a summons or issuing or enforcing a subpoena issued by another state or government entity in furtherance of such laws).
[6] Health-General §4-302.5(d)(1)

EHRA
HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

350 North Orleans Street, Suite S10000
Chicago, IL 60654

@EHRAssociation | ehra.org

October 4, 2023

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

RE: Feedback on proposed amendments COMAR 10.25.07 and 10.25.18

Dear Executive Director Steffen and the Maryland Health Care Commission,

The HIMSS Electronic Health Record (EHR) Association is pleased to have an opportunity to provide feedback on proposed draft amendments:

> COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses
> COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information

As the national trade association of EHR developers, EHR Association member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States. Together, we work to improve the quality and efficiency of care through the adoption and use of innovative, interoperable, and secure health information technology.

The inclusion of developers of certified health IT in Maryland's definition of a health information exchange (HIE) creates many of the issues identified in our comments below. Responsibilities that may be appropriate for an HIE that maintains a central repository of data being transacted, such as auditing the transactions or reviewing storage capacity, are infeasible and entirely out of the scope of responsibilities for a developer of certified health IT whose job is instead to author software that is deployed and maintained by a healthcare organization. Developers do not control the configuration and deployment of the software by healthcare organizations, do not make hardware purchasing decisions for healthcare organizations, and do not have the right to audit transactions within a healthcare organization's software. Maryland's policies would be better served by identifying the expectations for an HIE organization (which might dictate exchange policies, directly monitor exchange traffic, control hardware used in exchange, and have direct interaction with patients) separate from the expectations of developers of certified health IT, including electronic health records, which should focus on the provision of interoperability-capable software to Maryland providers who license it.

As we have previously written to you, the new Maryland legislation requiring the filtering and segmentation of reproductive health information does not align with the current capabilities of certified electronic health records in use in Maryland, and there is insufficient time between the enactment of SB 0786 and the December 1, 2023, effective date for the development of new features. We recognize the challenge in which the MHCC finds itself in being tasked to implement a law with an unrealistic effective date outlined in statute, but we want to be clear that that timeline is infeasible for most software developers.

The EHR Association has long explained to regulators at the Federal and State levels that 18-24 months should be allowed for the development of new EHR features after standards for that development have reached sufficient maturity for adoption. The current timeline allows for six months between the enactment of SB 0786 and required compliance. Even with the additional few months before penalties begin, this is not adequate time. Additionally, data segmentation and consent technical standards such as might be used to support Maryland's goal of restricting the sharing of sensitive reproductive health information are not sufficiently mature through the industry's standards adoption process at this time. The 18–24-month time period necessary for the development, testing, and implementation of these functionalities and standards cannot begin until that work is complete; the State should seek to work with standards development organizations and other industry stakeholders to help drive sufficient maturity for these standards to support these use cases.

We have provided detailed feedback in the attached table.

Thank you for your consideration,

David J. Bucciferro
Chair, EHR Association
Foothold Technology

William J. Hayes, M.D., M.B.A.
Vice Chair, EHR Association
CPSI

HIMSS EHR Association Executive Committee

Leigh Burchell
Altera Digital Health

Barbara Hobbs
MEDITECH, Inc.

Cherie Holmes-Henry
NextGen Healthcare

Stephanie Jamison
Greenway Health

Ida Mantashi
Modernizing Medicine

Kayla Thomas
Oracle Cerner

MHCC Commission Meeting Agenda, December 15, 2005 (maryland.gov)

Title 10 MARYLAND DEPARTMENT OF HEALTH Subtitle 25 MARYLAND HEALTH CARE COMMISSION

Chapter 18 Health Information Exchanges: Privacy and Security of Protected Health Information

Row	Section	Text	EHRA Comment
1	Chapter 18.01 B(1)	(1) [A health information exchange] An HIE, as defined in Regulation .02B(28) of this chapter[;] including: (a) An individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that allows, enables, or requires the use of any technology or services for access, exchange, or use of electronic protected health information: (i) Among more than two unaffiliated individuals or entities that are enables to exchange electronic protected health information with each other; and (ii) That is for a treatment, payment, or health care operations purpose, as those terms are defined in 45 C.F.R §164.501, regardless of whether the individuals or entities are subject to the requirements of 45 CFR parts 160 and 164; (b) A health information technology developer of certified health information technology, as that term is defined in Regulation .02B(36) of this chapter;	The roles of traditional health information exchanges (such as ONC refers to as HIEs or HINs) is very different than the role of a developer of certified health information technology, and the conflation of the two definitions here causes problems throughout several related Maryland regulations. Many of the requirements previously applied to HIEs being inapplicable to the role of a software development company that provides software (which may or may not include interoperability capabilities) but may not control the use of the software by healthcare organizations, including aspects such as storage and hardware capacity, user provisioning, patient education, capture of applicable patient consents, auditing of inappropriate use, and user deprovisioning. We suggest that Maryland separately identify the expectations for an HIE (which might dictate exchange policies, directly monitor exchange traffic, control hardware used in exchange, and have direct interaction with patients) from the expectations of developers of certified health IT, which should focus on provision of interoperability-capable software to Maryland providers who license it.
2	Chapter 18.01 D	D. In the event that an HIE is unable to meet a requirement of this chapter independently, it may do so by the execution of a written agreement or by requesting an exemption in accordance with Regulation. 09(G) or (H) of this chapter.	Given the discrepancy in definitions identified in Row 1 above, the ability to request an exemption will be critical for certified health IT developers who do not perform the roles of an HIE and for whom many sections of this regulation likely will not be inapplicable.
3	Chapter 18.02 B(40)	(40) “Legally protected health information” means the health information subject to restrictions	Health IT developers will require more specificity as to how this information will be defined and provided to design

		under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.	software solutions that will support Maryland providers, including: 1. What code sets will be used? 2. Where will codes be published? 3. How often will codes be updated? 4. What are expectations for uncoded data, such as free text notes? We suggest the following addition in bold and italics to clarify that legally protected health information is care delivered in Maryland: (40) "Legally protected health information" means the health information ***about care delivered and received in Maryland after December 1, 2023*** subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.
4	Chapter 18.03 B(4)-(6)	(4) An HIE shall make health care consumer educational materials readily available, at no charge, to participating organizations and [their users] the participating organizations' users through distribution channels such as websites, postal mail, email, secure third-party smart phone applications, and any other reasonable media or distribution channel commonly used and generally available to the HIE and health care consumer. (5) In addition to the foregoing requirements, with regard to sensitive health information, the health care consumer educational content shall include: (a) The scope	We suggest that educational obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT are unlikely to have direct relationships with patients or consumers. Patient education on health data exchange (and other similar topics) is conducted by healthcare providers who have a relationship with the patient and can contextualize what exchange consents might mean. Some healthcare organizations may vary in how they operationalize a patient's right to opt in or out of use of

		of sensitive health information; (b) The health care consumer's right to control sensitive health information; (c) The method by which to engage in the granular patient consent process; (d) The method(s) by which the health care consumer can access the patient's own sensitive health information; (e) The circumstances under which an HIE must restrict or may disclose legally protected health information; and (f) The method by which a health care consumer can request that a patient's legally protected health information be disclosed to a specific health care provider; (6) When an HIE updates its health care consumer educational content, the HIE shall timely make the updated materials available to health care consumers	interoperability features, which also makes it important that such education comes from the healthcare provider, and not generically from a software developer.
5	Chapter 18.04 A(3)(b)	(b) If federal or State law does not require written consent or authorization for access, use, or disclosure of sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE.	Developers of certified health IT are not in a position to dictate the consent policies of healthcare providers who use their software, and those healthcare providers may be considering not only federal and state law, but also the policies of other exchanges they participate in and their patient's preferences. It is not feasible for a developer of certified health IT to guarantee that no users of its software ask for consent in cases where it is not required by federal or state law.
6	Chapter 18.04 C	C. Procedures for disclosing or re-disclosing legally protected health information. (1) An HIE shall be in compliance with Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX. (2) By December 18,2023, an HIE shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law; or (b) An implementation plan that includes: (i)	Developers of certified health IT will not be able to make the affirmation described because it includes multiple components outside of their control and role. It is critical to rephrase the affirmation in (a) and (b) to better match the role of a developer of certified health IT, recognizing that the developer of the software cannot force healthcare provider organizations to install

		An affirmation that despite its best efforts, the HIE lacks the technological capability to fully comply with §C(1) of this regulation as of December 1, 2023, including a detailed explanation of the HIE's limitations; (ii) A detailed description of the steps the HIE is taking to ensure compliance with §C(1) of this regulation by June 1, 2024; (iii) A timeline to implement the requirements Health-General Article § 4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX by June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan. (3) If an HIE submits an implementation plan in accordance with §C(2)(b), the HIE shall: (a) Notify all participating organizations by December 18, 2023 that the HIE is unable to comply with §C(1) with a written notice that describes the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan; (b) Provide a status report to the Commission by April 1, 2024 detailing the progress the HIE has made under its implementation plan; and (c) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law.	software updates or use particular features of the software: "(a) An affirmation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or (b) An implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024." The short time period between the publication of these requirements (summer 2023) and the compliance deadline (December 2023 and June 2024) does not permit sufficient time for the development of new certified health IT features. EHRA members require 18-24 months to develop new features after national standards are mature; the lack of standards maturity for data segmentation capabilities means even more time for the development of such features will likely be necessary in this case. Developers of certified health IT will need further time beyond June 1, 2024, to safely develop and deliver data segmentation features to Maryland healthcare organizations. Similarly, healthcare organizations have varying paces for installing updates and upgrades to their health IT. Some healthcare organizations may upgrade once a year. If an organization typically upgrades in the spring, and then a software developer releases new features supporting data segmentation in the summer, the healthcare organization may not have those features in use until the following spring. Maryland healthcare providers will also need further time beyond June

			1, 2024, to implement and use new data segmentation features.
7	Chapter 18.06 A(3)-(4)	(3) [At least monthly, conduct] Conduct random audits of the user access logs to identify any unusual finding; and, if the HIE has been notified about an unusual finding or has reason to believe that inappropriate access has occurred, [more frequently than monthly.] conduct random audits at least every other week until the unusual finding or inappropriate access has been mitigated; (4) At least quarterly, conducted random audits of security measures and any other forms of data security in place to determine if they are still sufficient and compliant with applicable standards;	We suggest that auditing obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT are not in a position to audit (random or quarterly) certified health IT audit logs when the technology is deployed by healthcare organizations. Healthcare organization administrators are responsible for monitoring their own health IT audit logs.
8	Chapter 18.06 A(7)(a)	(a) If the unusual finding involves fewer than 10 patients, [in a timely manner] within 5 business days after the unusual findings is discovered;	We suggest that notification obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Notifications of unusual findings in the logs of a certified health IT module would be handled by the healthcare organization using the software.
9	Chapter 18.06 A(8)(b)	(b) The HIE shall perform periodic testing and implement upgrades and updates to ensure that the storage medium is secure and has not been improperly accessed.	We suggest that storage obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT do not control the hardware on which healthcare organizations decide to deploy.
10	Chapter 18.06 C (1)-(2)	C. An HIE shall [conduct an annual] at least annually enlist a qualified independent auditing firm to audit its privacy, [and] security, and legal [audit in] compliance in accordance with the following provisions. (1) The audit shall [be aimed at detecting patterns of inappropriate access, use, maintenance, and disclosure of information that are in	We suggest that auditing obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT do not have the right to audit software in live use by their customers; audits would be engaged and conducted by the healthcare provider organizations.

		violation of this chapter;]: (a) Assess potential risks to protect the confidentiality, integrity, and security of PHI; (b) Assess operational compliance with State and federal law, including the requirements of this Chapter; (c) Be designed to determine the adequacy of business and technology-related controls, policies, and procedure and other safeguards employed by third-party service organizations based on industry standards and best practices; and (d) Include an assessment of cybersecurity posture and compliance with this Chapter, applicable provisions in HIPAA and HITECH, and recognized security practices by way of accreditation or certification from a nationally recognized entity. (2) An HIE shall develop auditing policies and procedures for the independent auditor to conduct such an audit, which shall include, at a minimum: (a) The scope of the audit; (b) A description of all third-party organizations and processes to review and assess related privacy and security controls and audit reports; (c) Interviews with relevant staff, including those from third party service organizations, as appropriate; (d) Names and contact information of all persons responsible for reviewing and maintaining privacy and security to include the implementation of corrective actions to address apparent gaps; and (e) Timeframes for completing audits and related activities.	
11	Chapter 18.06 D	D. Upon the request of the Commission and consistent with the specifications in such request, an HIE shall: (1) Provide a summary of the results of any audit that is required by this chapter, and any [supporting documentation] corrective action plans identified by the audit, to the Commission; and (2) Conduct an	We suggest that auditing obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT do not have the right to audit software in live use by their customers; audits would be engaged and conducted by the healthcare provider organizations.

		additional unscheduled audit within 180 days of the request and provide the results of such an audit to the Commission within the time frame specified by the Commission.	
12	Chapter 18.06 F	F. If an HIE's audit reveals information that demonstrates a pattern of noncompliance with State and federal law, then: (1) The HIE shall use the findings from the audit to: (a) Educate and train all impacted persons, which may include its workforce, participating organizations, and authorized users, on proper access, use, and disclosure of information through or from the HIE; and (b) Evaluate and implement new control measures, including policies, procedures, or technology, to ensure compliance. (2) The HIE shall take the appropriate measures specified in the Regulation. 07 of this Chapter.	We suggest that auditing obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1. Developers of certified health IT do not have the right to audit software in live use by their customers; audits would be engaged and conducted by the healthcare provider organizations.
13	Chapter 18.07 C	C. If an HIE has a reasonable belief that a breach or non-HIPAA violation has occurred, either as a result of an investigation or otherwise, the HIE shall (1) For a breach, follow Regulation .08 of this chapter and federal breach notification requirements and timelines; (2) For non-HIPAA violations, submit a corrective action plan to the Commission within 10 business days of conclusion of its investigation, which shall include: (a) Any remedial action necessary to address the breach or violation as soon as practicable; (b) any steps necessary to correct the underlying problem, such as a change in processes or procedures, new technology, and training and (c) An appropriate and reasonable time frame for implementing the remedial action. (3) Within a reasonable time frame, but in no event more than 10 business days following the investigation, provide the following	We suggest that breach notification obligations be removed from developers of certified health IT, as breach notification and other notification obligations under HIPAA will already be addressed between developers of certified health IT and healthcare providers in their business associate agreements.

		to the Commission, and to the participating organizations: (a) A copy of the findings of the investigation, excluding any PHI or sensitive health information; (b) Each remedial action to be taken by each person and the associated time frame of the remedial action; (c) Any action necessary to mitigate the harm that may be caused by the breach or the non-HIPAA violation; (d) The identity of the person that is responsible for carrying out each action to mitigate harm; and (e) Any future action that the HIE may take, including suspension of access or progressive discipline, if [the] a person does not comply with the remedial action.	
14	Chapter 18.09 C(3)	(3) Civil and criminal penalties. (a) Civil penalties. A person who knowingly fails to comply with this chapter shall be subject to a civil penalty not exceeding $10,000 per day for each person impacted by the non-compliance based on: (i) The extent of actual or potential public harm caused by the violation; (ii) The cost of the investigation; and (iii) The person's prior record of compliance. (b) Criminal penalties. Beginning June 1, 2024, a person who knowingly violates Health-General Article, §4-302.5, Annotated Code of Maryland, shall be guilty of a misdemeanor and on conviction is subject to a fine not to exceed $10,000 per day based on: (i) The extent of actual or potential public harm caused by the violation; (ii) The cost of the investigation; and (iii) The person's prior record of compliance.	The short time period between the publication of these requirements (summer 2023) and the compliance deadlines (December 2023 and June 2024) does not permit sufficient time for the development of new certified health IT features. EHRA members require 18-24 months to develop new features after national standards are mature; the lack of standards maturity for data segmentation capabilities means even more time for the development of such features will likely be necessary in this case. Developers of certified health IT will need further time beyond June 1, 2024, to safely develop and deliver data segmentation features to Maryland healthcare organizations. Similarly, healthcare organizations have varying paces for installing updates and upgrades to their health IT. Some healthcare organizations may upgrade once a year. If an organization typically upgrades in the spring, and then a software developer releases new features supporting data segmentation

			in the summer, the healthcare organization may not have those features in use until the following spring. Maryland healthcare providers will also need further time beyond June 1, 2024, to implement and use new data segmentation features.

MHCC Commission Meeting Agenda, December 15, 2005 (maryland.gov)

Title 10 MARYLAND DEPARTMENT OF HEALTH Subtitle 25 MARYLAND HEALTH CARE COMMISSION Chapter 07 Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses

Row	Section	Text	Comment
16	Chapter 07.02 B.(8)	(8) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including (a) Mifepristone data, as defined by the Secretary, and (b) As provided in COMAR XX.XX.XXX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.	Health IT developers will require more specificity as to how this information will be defined and provided to design software solutions that will support Maryland providers, including: 1. What code sets will be used? 2. Where will codes be published? 3. How often will codes be updated? 4. What are expectations for uncoded data, such as free text notes? We suggest the following addition in bold and italics to clarify that legally protected health information is care delivered in Maryland: (40) "Legally protected health information" means the health information ***about care delivered and received in Maryland after December 1, 2023*** subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-

			301, Annotated Code of Maryland.
17	Chapter 07.05 A.(2)(c)	(c) Provide an attestation signed by an officer of the applicant that the applicant restricts disclosure of legally protected health information as required by Health-General Article, §4-302.5, Annotated and COMAR XX.XX.XX;	Developers of certified health IT will not be able to make the attestation described because it includes multiple components outside of their control and role. It is critical to rephrase the attestation to better match the role of a developer of certified health IT, recognizing that the developer of the software cannot force healthcare provider organizations to install software updates or use particular features of the software: "(C) Provide an attestation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or an implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."
18	Chapter 09	B. An MHCC-Certified EHN must report on compliance progress to the Commission. (1) By December 18, 2023, an MHCC-certified EHN shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX; or (b) An implementation plan that includes: (i) An affirmation that despite its best efforts, the MHCC-certified EHN lacks the technological capability to fully comply with Health-General Article, §4-302.5, Annotated Code of Maryland as of December 1, 2023, including a detailed explanation of the EHN's limitations; (ii) A detailed description	Developers of certified health IT will not be able to make the affirmation described because it includes multiple components outside of their control and role. It is critical to rephrase the affirmation to better match the role of a developer of certified health IT, recognizing that the developer of the software cannot force healthcare provider organizations to install software updates or use particular features of the software: "(a) An affirmation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or (b) an implementation plan that includes a description of the steps the certified

		of the steps the MHCC-certified EHN is taking to ensure compliance with Health-General Article, §4-302.5, Annotated Code of Maryland by June 1, 2024; (iii) A timeline to implement Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX Aby June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted by the MHCC-certified EHN during the implementation of its plan. (2)If a MHCC-certified EHN submits an implementation plan in accordance with §B(1), the EHN shall: (a) Provide a status report to the Commission by April 1, 2024 detailing the progress the MHCC-certified EHN has made under its implementation plan; and (b) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law. C. Beginning June 1, 2024, a person who knowingly violates Health-General Article, §4-302.5, Annotated Code of Maryland, shall be guilty of a misdemeanor and on conviction is subject to a fine not to exceed $10,000 per day based on: (1) The extent of actual or potential public harm caused by the violation; (2) The cost of investigating the violation; and (3) The person's prior record of compliance.	health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."

Epic

October 4, 2023

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

RE: Feedback on proposed amendments to COMAR 10.25.07 and 10.25.18

Dear Executive Director Steffen and the Maryland Health Care Commission,

Thank you for the opportunity to share informal comments on proposed amendments to 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 in advance of the Maryland Health Care Commission's (MHCC) October 19th meeting.

We are concerned that MHCC is expecting developers to attest to activities we do not control. As background, Epic develops standards-based software that is licensed to and locally configured and deployed by more than 50 organizations providing care in Maryland. Each of those organizations establishes their own policies and procedures to control their usage of the software, including the exchange of patient records with other providers. Records that are exchanged by users of Epic's standards-based software are exchanged directly among exchange partners; they do not route through a central system under Epic's control, nor are Epic staff involved in the transactions.

In its proposal, by defining developers of certified health IT as health information exchanges, MHCC is asking developers of health IT to bear responsibility for patient education, audit monitoring, consent capture, investigation of suspicious activity, user deprovisioning, and hardware capacity planning. Each of these activities is entirely a responsibility of our customer healthcare organizations.

MHCC should revise its proposed regulations to require developers to bear responsibility only for activities under their control. Specifically, expectations for developers of health information technology should focus on their software meeting specific interoperability standards. Developers cannot be responsible for configuration decisions made by healthcare organizations that deploy our software nor for the behavior of clinicians and patients who use the software.

MHCC is also proposing new regulations implementing recently passed legislation to protect reproductive health information. We agree that patient and caregiver information related to the provision or receipt of legal reproductive care should be kept private. Earlier this year, we commented in support of the US Department of Health and Human Services' Office for Civil Rights proposal to modify HIPAA to strengthen HIPAA's protections for reproductive health information, including a prohibition on regulated entities disclosing patient reproductive health information for the purposes of certain criminal, civil, or administrative investigations and proceedings. We believe this approach preserves the ability for regulated entities to continue using and exchanging health information appropriately while setting a higher bar for disclosures of the information for purposes unrelated to the provision of safe, high-quality patient care.

As Maryland continues its efforts to protect patient privacy with respect to legally protected health care, we encourage significantly more time for development of new software features by software developers and deployment of that new software by the organizations that license and use it. We caution that that the best approach to protect privacy and patient safety is actively evolving, and we encourage Maryland to allow further progress of national standards so that Maryland's approach is aligned.

In the table below, we have provided examples of where COMAR 10.25.07 and 10.25.18 can be edited to address these issues and facilitate the best care for the patients of Maryland.

Thank you for your consideration,

Sasha TerMaat
Epic

Section	Ch 18 Health Information Exchanges: Privacy and Security of Protected Health Information	Epic Feedback
18.01 B(1)	(1) [A health information exchange] An HIE, as defined in Regulation .02B(28) of this chapter[;] including: (a) An individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that allows, enables, or requires the use of any technology or services for access, exchange, or use of electronic protected health information: (i) Among more than two unaffiliated individuals or entities that are enables to exchange electronic protected health information with each other; and (ii) That is for a treatment, payment, or health care operations purpose, as those terms are defined in 45 C.F.R §164.501, regardless of whether the individuals or entities are subject to the requirements of 45 CFR parts 160 and 164; (b) A health information technology developer of certified health information technology, as that term is defined in Regulation .02B(36) of this chapter;	Maryland's inclusion of developers of health IT certified through the Office of the National Coordinator's program in the definition of HIE places Epic and other health IT developers in an impossible situation of being asked to attest to activities that they do not control. Expectations for developers of health information technology should focus on provision of software meeting specific interoperability standards.
18.01 D	D. In the event that an HIE is unable to meet a requirement of this chapter independently, it may do so by the execution of a written agreement or by requesting an exemption in accordance with Regulation. 09(G) or (H) of this chapter.	Developers will critically need exceptions because many of the expectations for HIEs are outside of a developer's control.
18.02 B(40)	(40) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.	We suggest the following addition (in italics) to clarify that legally protected health information is care delivered in Maryland: (40) "Legally protected health information" means the health information *about care delivered and received in Maryland after December 1, 2023,* subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.
18.03 B(4)-(6)	(4) An HIE shall make health care consumer educational materials readily available, at no charge, to participating organizations and [their users] the participating organizations' users through distribution channels such as websites, postal mail, email, secure third party smart phone applications, and any other reasonable media or distribution channel commonly used and generally available to the HIE and health care consumer. (5) In addition to the foregoing requirements, with regard to sensitive health information, the health care consumer educational content shall include: (a) The scope of sensitive health information; (b) The health care consumer's right to control sensitive health information; (c) The method by which to engage in the granular patient consent process; (d) The method(s)	Patient education is best performed by a healthcare-providing organization that maintains relationships with patients and can offer specificity on their organization's configuration and policies for information-sharing and authorization/consent. Software developers should not be forced to intrude on the relationship between patients and their healthcare providers. We suggest that educational obligations not apply to

Section	Ch 18 Health Information Exchanges: Privacy and Security of Protected Health Information	Epic Feedback
	by which the health care consumer can access the patient's own sensitive health information; (e) The circumstances under which an HIE must restrict or may disclose legally protected health information; and (f) The method by which a health care consumer can request that a patient's legally protected health information be disclosed to a specific health care provider; (6) When an HIE updates its health care consumer educational content, the HIE shall timely make the updated materials available to health care consumers	developers of certified health IT.
18.04 A(3)(b)	(b) If federal or State law does not require written consent or authorization for access, use, or disclosure of sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE.	Healthcare organizations may ask patients for authorization/consent to share their information for multiple reasons, including the policies of other HIEs they participate in. They often do this to foster a sense of trust with their patients, and to provide transparency for patients about how their information is disclosed. Seeking patient consent to exchange information should not be prohibited.
18.04 C	C. Procedures for disclosing or re-disclosing legally protected health information. (1) An HIE shall be in compliance with Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX. (2) By December 18,2023, an HIE shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law; or (b) An implementation plan that includes: (i) An affirmation that despite its best efforts, the HIE lacks the technological capability to fully comply with §C(1) of this regulation as of December 1, 2023, including a detailed explanation of the HIE's limitations; (ii) A detailed description of the steps the HIE is taking to ensure compliance with §C(1) of this regulation by June 1, 2024; (iii) A timeline to implement the requirements Health-General Article § 4-302.5, Annotated Code of Maryland and COMAR XX.XX.XXX by June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan. (3) If an HIE submits an implementation plan in accordance with §C(2)(b), the HIE shall: (a) Notify all participating organizations by December 18, 2023 that the HIE is unable to comply with §C(1) with a written notice that describes the extent legally protected health information and other health information will be restricted through the HIE during the implementation of its plan; (b) Provide a status report to the Commission by April 1, 2024 detailing the progress the HIE has made under its implementation plan; and (c) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law.	The proposed affirmation is drafted from the perspective of an entity that controls technology as deployed, not from the perspective of a developer that licenses technology that is ultimately deployed and configured by another party. Developers will not be able and should not be expected to make the affirmation proposed. The affirmation will need to be revised to account for use and deployment of the software beyond a developer's control, in the following way (for example): "(a) An affirmation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or (b) An implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."
18.06 A(3)-(4)	(3) [At least monthly, conduct] Conduct random audits of the user access logs to identify any unusual finding; and, if the HIE has been notified about an unusual finding or has reason to believe that inappropriate access has occurred, [more frequently than monthly.] conduct random audits at least every other week until the unusual finding or inappropriate access has	Developers may not have the right to audit use of their software by the organizations that license it; healthcare organization administrators audit their own usage. We suggest that auditing obligations be removed from developers of

Section	Ch 18 Health Information Exchanges: Privacy and Security of Protected Health Information	Epic Feedback
	been mitigated; (4) At least quarterly, conducted random audits of security measures and any other forms of data security in place to determine if they are still sufficient and compliant with applicable standards;	certified health IT.
18.06 A(7)(a)	(a) If the unusual finding involves fewer than 10 patients, [in a timely manner] within 5 business days after the unusual findings is discovered;	Notifications regarding unusual findings would be handled by the healthcare organization administrators who monitor the software usage. We suggest that notification obligations be removed from developers of certified health IT.
18.06 A(8)(b)	(b) The HIE shall perform periodic testing and implement upgrades and updates to ensure that the storage medium is secure and has not been improperly accessed.	Developers are not maintaining storage for locally deployed software; this obligation should be removed.
18.06 C (1)-(2)	C. An HIE shall [conduct an annual] at least annually enlist a qualified independent auditing firm to audit its privacy, [and] security, and legal [audit in] compliance in accordance with the following provisions. (1) The audit shall [be aimed at detecting patterns of inappropriate access, use, maintenance, and disclosure of information that are in violation of this chapter;]: (a) Assess potential risks to protect the confidentiality, integrity, and security of PHI; (b) Assess operational compliance with State and federal law, including the requirements of this Chapter; (c) Be designed to determine the adequacy of business and technology-related controls, policies, and procedure and other safeguards employed by third-party service organizations based on industry standards and best practices; and (d) Include an assessment of cybersecurity posture and compliance with this Chapter, applicable provisions in HIPAA and HITECH, and recognized security practices by way of accreditation or certification from a nationally recognized entity. (2) An HIE shall develop auditing policies and procedures for the independent auditor to conduct such an audit, which shall include, at a minimum: (a) The scope of the audit; (b) A description of all third-party organizations and processes to review and assess related privacy and security controls and audit reports; (c) Interviews with relevant staff, including those from third party service organizations, as appropriate; (d) Names and contact information of all persons responsible for reviewing and maintaining privacy and security to include the implementation of corrective actions to address apparent gaps; and (e) Timeframes for completing audits and related activities.	Developers may not have the right to audit use of their software by the organizations that license it; healthcare organization administrators audit their own usage We suggest that auditing obligations be removed from developers of certified health IT.
18.06 D	D. Upon the request of the Commission and consistent with the specifications in such request, an HIE shall: (1) Provide a summary of the results of any audit that is required by this chapter, and any [supporting documentation] corrective action plans identified by the audit, to the Commission; and (2) Conduct an additional unscheduled audit within 180 days of the request and provide the results of such an audit to the Commission within the time frame specified by the Commission.	Developers may not have the right to audit use of their software by the organizations that license it; healthcare organization administrators audit their own usage We suggest that auditing obligations be removed from developers of certified health IT.
18.06 F	F. If an HIE's audit reveals information that demonstrates a pattern of noncompliance with State and federal law, then: (1) The HIE shall use the findings from the audit to: (a) Educate	Developers may not have the right to audit use of their software by the organizations that license it; healthcare

Section	Ch 18 Health Information Exchanges: Privacy and Security of Protected Health Information	Epic Feedback
	and train all impacted persons, which may include its workforce, participating organizations, and authorized users, on proper access, use, and disclosure of information through or from the HIE; and (b) Evaluate and implement new control measures, including policies, procedures, or technology, to ensure compliance. (2) The HIE shall take the appropriate measures specified in the Regulation. 07 of this Chapter.	organization administrators audit their own usage We suggest that auditing obligations be removed from developers of certified health IT.
18.07 C	C. If an HIE has a reasonable belief that a breach or non-HIPAA violation has occurred, either as a result of an investigation or otherwise, the HIE shall (1) For a breach, follow Regulation .08 of this chapter and federal breach notification requirements and timelines; (2) For non-HIPAA violations, submit a corrective action plan to the Commission within 10 business days of conclusion of its investigation, which shall include: (a) Any remedial action necessary to address the breach or violation as soon as practicable; (b) any steps necessary to correct the underlying problem, such as a change in processes or procedures, new technology, and training and (c) An appropriate and reasonable time frame for implementing the remedial action. (3) Within a reasonable time frame, but in no event more than 10 business days following the investigation, provide the following to the Commission, and to the participating organizations: (a) A copy of the findings of the investigation, excluding any PHI or sensitive health information; (b) Each remedial action to be taken by each person and the associated time frame of the remedial action; (c) Any action necessary to mitigate the harm that may be caused by the breach or the non-HIPAA violation; (d) The identity of the person that is responsible for carrying out each action to mitigate harm; and (e) Any future action that the HIE may take, including suspension of access or progressive discipline, if [the] a person does not comply with the remedial action.	Corrective action plans would be handled by the healthcare organization administrators who monitor the software usage and handles user provisioning. We suggest that these obligations be removed from developers of certified health IT.

Section	Ch 07 Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses	Epic Feedback
07.02 B.(8)	(8) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including (a) Mifepristone data, as defined by the Secretary, and (b) As provided in COMAR XX.XX.XXX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.	We suggest the following addition (in italics) to clarify that legally protected health information is care delivered in Maryland: (40) "Legally protected health information" means the health information *about care delivered and received in Maryland after December 1, 2023* subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including: (a) Mifepristone data, as defined by the Secretary; and (b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.
07.05 A.(2)(c)	(c) Provide an attestation signed by an officer of the applicant that the applicant restricts disclosure of legally protected health information as required by Health-General Article, §4-302.5, Annotated and COMAR XX.XX.XX;	The proposed attestation is drafted from the perspective of an entity that controls technology as deployed, not from the perspective of a developer that licenses technology that is ultimately deployed and configured by another party. Developers will not be able and should not be expected to make the attestation proposed. The attestation will need to be revised to account for use and deployment of the software beyond a developer's control, in the following way (for example): "(C) Provide an attestation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or an implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."
09	B. An MHCC-Certified EHN must report on compliance progress to the Commission. (1) By December 18, 2023, an MHCC-certified EHN shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure	The proposed affirmation is drafted from the perspective of an entity that controls technology as deployed, not from the perspective of a developer that licenses technology that is

Section	Ch 07 Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses	Epic Feedback
	legally protected health information to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX; or (b) An implementation plan that includes: (i) An affirmation that despite its best efforts, the MHCC-certified EHN lacks the technological capability to fully comply with Health-General Article, §4-302.5, Annotated Code of Maryland as of December 1, 2023, including a detailed explanation of the EHN's limitations; (ii) A detailed description of the steps the MHCC-certified EHN is taking to ensure compliance with Health-General Article, §4-302.5, Annotated Code of Maryland by June 1, 2024; (iii) A timeline to implement Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX Aby June 1, 2024; and (iv) A description of the extent legally protected health information and other health information will be restricted by the MHCC-certified EHN during the implementation of its plan. (2)If a MHCC-certified EHN submits an implementation plan in accordance with §B(1), the EHN shall: (a) Provide a status report to the Commission by April 1, 2024 detailing the progress the MHCC-certified EHN has made under its implementation plan; and (b) Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law. C. Beginning June 1, 2024, a person who knowingly violates Health-General Article, §4-302.5, Annotated Code of Maryland, shall be guilty of a misdemeanor and on conviction is subject to a fine not to exceed $10,000 per day based on: (1) The extent of actual or potential public harm caused by the violation; (2) The cost of investigating the violation; and (3) The person's prior record of compliance.	ultimately deployed and configured by another party. Developers will not be able and should not be expected to make the affirmation proposed. The affirmation will need to be revised to account for use and deployment of the software beyond a developer's control, in the following way (for example): "(a) An affirmation that it provides to its Maryland users software that includes the capability for them to filter or restrict from disclosure information they identify as legally protected in their jurisdiction or (b) an implementation plan that includes a description of the steps the certified health IT developer is taking to provide its Maryland users with software that includes this capability by June 1, 2024."

Greenway Health™

October 4, 2023

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

RE: Feedback on proposed amendments COMAR 10.25.07 and 10.25.18

Dear Executive Director Steffen and the Maryland Health Care Commission,

Greenway Health appreciates the opportunity to respond to Maryland's proposed amendments for 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*.

Greenway is proud to serve provider practices of all sizes in more than 40 specialties with our electronic health record (EHR) offerings, practice management solutions and revenue cycle management services. Greenway Health is also a founding member, and active participant, in the national trade association of EHR developers. The EHR Association member companies serve the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States.

These comments we offer today on behalf of Greenway Health largely echo the Electronic Health Record Association's (EHRA) letter that was thoughtfully composed and approved by all members of the EHRA, as we unanimously work to tackle the unique challenges set forth by Maryland in existing legislation that defines developers of federally certified health IT as "health information exchanges (HIEs)" in Maryland. We know many of the points that all EHR developers have made in the prior years have been carefully considered by the Maryland Health Care Commission; we offer these comments below and urge the Commission to review the entirety of EHRAs letter for additional important details.

We join the EHRA in suggesting that Maryland separately identify the expectations for an HIE from the expectations of developers of certified health IT that focus on providing of interoperability-capable software to Maryland providers who license it and do not have the ability or authority to control or oversee things like consent policies in individual practices, nor audit functions.

We are concerned that the responsibilities placed on HIEs under the proposed amendments create a conflict with our existing legal and contractual responsibilities as a HIPAA business associate to our covered entity clients. As a developer of certified health IT, Greenway provides the EHR software but does not control the flow of data into or out of each client's EHR. The HIPAA Privacy Rule permits a business associate of a HIPAA covered entity to use and disclose PHI only pursuant to the explicit terms of a business associate agreement as required under 45 CFR 164.502(e)(2). Such business associate agreements do not permit Greenway to control our clients' exchange of PHI, directly monitor exchange traffic, have direct interaction with patients, or audit our client's user access logs.

Finally, we urge Maryland to consider that data segmentation capabilities like the ones that are being requested as a result of the passage of SB 0786 exceed federal requirements and the timelines for implementation of these new functionalities are insufficient for nearly all EHR

Greenway Health™

developers to attain. EHRA members require 18-24 months for the development, testing, and implementation of new functionalities, therefore, developers of certified health IT will need further time beyond June 1, 2024, to safely develop and deliver data segmentation features to Maryland healthcare organizations.

Sincerely,

Karen W. Mulroe
General Counsel

JOHNS HOPKINS
UNIVERSITY & MEDICINE

October 4, 2023

Via email to Anna.gribble1@maryland.gov

Maryland Health Care Commission
Attn: Anna Gribble
Center for Health Information Technology and Innovative Care Delivery
4160 Patterson Ave.
Baltimore, MD 21215

RE: Preliminary Review: Draft Amendments to COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information

On behalf of The Johns Hopkins Health System Corporation and The Johns Hopkins University ("Johns Hopkins"), we write to provide informal comments to the proposed emergency regulations COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information ("Proposed Regulations") issued by the Maryland health Care Commission ("MHCC") to implement Senate Bill 786, Health – Reproductive Health Services – Protected Information and Insurance Requirements (the "Act").

Johns Hopkins welcomes the opportunity to provide informal comments to the MHCC and encourages adoption of the proposals below in order to provide much needed clarity to health care providers and Health Information Exchanges ("HIEs") that operate in Maryland, and minimize any unintended consequences of the Act.

A. General Considerations

Johns Hopkins is one of the country's leading providers of women's health care. It provides comprehensive OBGYN services in multiple states, including providing abortion services in Maryland. In addition, Johns Hopkins is the largest provider of health care in the state of Maryland spanning care over 15 different specialties, including emergency services. As a result, the Act and the Proposed Regulations are likely to have a significant impact on Johns Hopkins patients who have received or will receive legally protected health care services.

Johns Hopkins supports the general policy of the Act and the proposed emergency regulations. We agree that protecting the confidentiality of patients and ensuring patients can receive legally protected health care without fear of prosecution is critical. We, however, believe that, as drafted, the Act and proposed emergency regulations will have significant unintended consequences that may significantly impair a woman's ability to obtain comprehensive health care in Maryland.

Johns Hopkins uses Epic as its Electronic Medical Record ("EMR") system. Epic governs CareEverywhere, which is an HIE integrated in the EMR system that allows clinicians to exchange medical record information in real time with other health care providers within Maryland and throughout the country. Using CareEverywhere has become commonplace for most providers and serves as a virtually seamless way for providers to gather accurate and complete medical record information on patients who they are treating.

Due to the way EMRs and CareEverywhere are structured, there is no current mechanism to segment unstructured data from being shared through CareEverywhere. Accordingly, significant changes to provider

documentation practices will likely need to be implemented in order to make data segmentation a reality, increasing the already large documentation burden on health care providers. Regardless of any potential future state, it is virtually impossible, with currently available technology, to restrict all of a patient's legally protected health information from disclosure through an HIE for historical information while disclosing the remainder of the patient's record. In order to comply with the Act, patients who have or will receive legally protected health care will need to be fully opted out of participating in CareEverywhere. As a result, none of a woman's healthcare information (e.g., oncology, cardiology, etc.) will be available to any of her treating providers in advance of any patient care encounter where consent can be obtained. Such a result will severely limit a patient's ability to take advantage of the benefits HIEs, such as CareEverywhere, offer in receiving more comprehensive and accurate care.

As such, Johns Hopkins respectfully offers the following suggested changes to the proposed regulations in order to allow for CareEverywhere and other HIEs to continue to serve as a valuable tool in providing the highest level of health care to women in the State of Maryland, while honoring a patient's wishes to withhold such information from being provided through HIEs if a patient so chooses.

B. Specific Comments

Section	Section Title	Proposed Language	Comment
10.25.18.02B	Definitions	**Add new definition of "knowingly."** *"Knowingly means a person, at the time of making a disclosure, has actual knowledge that legally protected health information is being disclosed through an HIE and that this disclosure violates Health-General Article § 4-302.5, Annotated Code of Maryland.*	Given the significant penalties associated with failure to comply with COMAR 10.25.18, we believe it is important to clarify what the definition of "knowingly" is as it relates to these regulations.
10.25.18.02B	Definitions	**Add a new definition of "specific treating provider."** *"Specific treating provider" means a health care provider that a patient, or parent or guardian of a patient, gives consent to receive sensitive health information in accordance with COMAR 10.25.18.04.*	Add clarification that the term "specific treating provider" has the same meaning as a health care provider already defined in statute to enable a patient to provide consent to share her information. While CareEverywhere can limit disclosure to a specific health care organization pursuant to consent, it cannot limit disclosure to, for example, one doctor. In order to permit any use of CareEverywhere by the impacted patients, a patient must be able to provide consent to release the information to an entire health care organization, if she

			chooses. It seems counter to the purpose of the Act for the legislature to not have intended to honor the wishes of the patient.
10.25.18.02B(40)	Definitions	**Modify the proposed definition of "Legally protected health information" as follows:** *(a) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including:* *(1) Mifepristone data, as defined by the Secretary, prescribed after June 24, 2022 to a patient located in the state of Maryland related to the diagnosis of medical termination of pregnancy; and* *(2) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes documented in structured data fields related to:* *(i) Abortion care provided in the state of Maryland after June 24, 2022; and* *(ii) Sensitive health services provided in the state of Maryland after June 24, 2022, as defined by Health-General, §4-301, Annotated Code of Maryland.* *(b) "Legally protected health information" does not include an electronic prescription and prescription related information transmitted to a pharmacy of the patient's choice.*	These clarifications are critical to ensuring the law can achieve its intended purpose without unfairly disadvantaging women from participation in HIEs. Given the intent of the Act, it is logical that the intent of the legislature was not to block legally protected health information received prior to the Supreme Court's decision in Dobbs, since such care would have been legal throughout the country. Additionally, the legislature's intent was to protect the right of women to receive legal reproductive care in Maryland, so the restrictions should be limited to care received in Maryland to avoid jurisdictional issues that may impact HIEs that operate across states. Finally, the suggested change related to structured data fields is consistent with the Acts reference to billing codes and is designed to address the concerns raised in our introduction related to the inability to segment data in unstructured text. Finally, e-prescribing in Maryland is done mostly through SureScripts, which is a registered HIE in the state of Maryland. We believe it is critical to be able to continue to offer the benefits of e-prescribing to patients

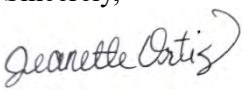
			without having to obtain full consent. Transmitting the prescription to the pharmacy of the patient's choice should not implicate the effects of the Act.
10.25.18.03A	Rights of a Health Care Consumer	**Insert new paragraph (5):** *(5) The right to control sensitive health information, including the right to give written consent in advance to disclosure of legally protected health information to one or more health care providers with whom the health care consumer may have a future provider-patient relationship.*	We think it is important for MHCC to clarify that health care consumers retain the right to decide to whom their information is disclosed and that this may include a patient wishing to sign a broad authorization in advance to permit the disclosure of her information through an HIE, so her treating providers have access to the information in advance of any in-person encounter.
10.25.18.04A(2)	Consent	**Add clarifying language to the consent requirements as follows:** *(2) If federal or State law requires written consent or authorization for access, use, or disclosure of sensitive health information, a person shall obtain consent or authorization consistent with the applicable law prior to the access, use, or disclosure of sensitive health information to and through an HIE to an authorized recipient, including as follows:* *(a) A patient, or parent or guardian of a patient, providing written consent to a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may specify:* *(i) Any health care provider to receive sensitive health information, at present or in the future, notwithstanding the existence of a current provider-patient relationship; and* *(ii) The duration of the consent, up to and including an unlimited period of time.*	Similar to the comment above, we believe clarification is needed from MHCC regarding how a patient can consent to have their sensitive information shared through an HIE. Of particular importance is honoring the wishes of the patient to choose to consent to the disclosure of information through an HIE to any provider she wishes and that such consent may include future providers whose names are not currently known. Such an approach is consistent with 42 CFR Part 2 where patients retain the right to choose how they wish for their sensitive information to be shared.

		(b) The consent obtained by a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may be revoked by the patient, or parent or guardian of a patient, at any time, upon reasonable notice.	
10.25.18.04A(3)	Emergency Exception	**Modify proposed changes to emergency exception as follows:** *(3) ~~[~~Notwithstanding §A(2) of this regulation, an HIE may transmit sensitive health information, in accordance with state and federal law, 42 CFR § 2.51and Health-General Article Title 4, Subtitle 3, Annotated Code of Maryland. [: (a) To medical personnel who have a need for information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention, as permitted by Part 2; and (b) In an emergency, if a health care provider makes a professional determination that an immediate disclosure is necessary to provide for the emergency health care needs of a patient or recipient.] ~~If federal or State law does not require written consent or authorization for access, use, or disclosure of sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE.~~*	As discussed above, consent will now need to be obtained from every woman who has received legally protected health care before for ANY of their health information can be shared through CareEverywhere. In emergency situations, it is unlikely such consent can be obtained. Additionally, the utility of an HIE tends to be most valuable in emergency situations where a patient is unable to relay clinically relevant history. As a result, we believe MHCC should retain the emergency exception under 10.25.18.04(A) and rely on the language in the Maryland Confidentiality of Medical Records Act ("MCMRA") in Md. Code, Health General § 4-305(b)(6) that permits the disclosure of medical records without the need for written patient authorization, ""[i]f a health care provider makes a professional determination that an immediate disclosure is necessary, to provide for the emergency health care needs of a patient or recipient."
10.25.18.09(C)(3)(a)	Enforcement	**Add clarifying language to the civil penalties** *Civil penalties. A person who knowingly fails to comply with this*	Add clarification that the civil penalties that can be assessed on HIEs are limited to those assessed

		chapter shall be subject to a civil penalty imposed by the Commission not exceeding $10,000 per day for each person impacted by the non-compliance based on:	by the Commission to confirm there is no private right of action under the regulations. Such an approach will ensure HIEs are more willing to work with the Commission to meet the purposes of the regulations without taking an overly conservative approach to ensure absolute compliance.

Thank you for your consideration. Please feel free to contact me at jortiz29@jhu.edu or 410.703.5352 or Pamela Rayne, Practice Group Leader & Chief Legal Counsel – Privacy Legal Department for Johns Hopkins Health System Corporation, at Prayne1@jhmi.edu or 410.614.9900 if you have any questions.

Sincerely,



Jeanette Ortiz
Deputy Director, Maryland State Affairs

cc: Pamela Rayne, Practice Group Leader & Chief Legal Counsel – Privacy Legal Department for Johns Hopkins Health System Corporation
Ben Steffen, Executive Director, MHCC
David Sharp, Director, Center for Health Information Technology and Innovative Care Delivery, MHCC
Alexa Bertinelli, Esq., Assistant Attorney General, MHCC
Caitlin E. Tepe, Esq., Assistant Attorney General, MHCC
Ruby Potter, Health Facilities Coordinator, MHCC

KAISER PERMANENTE®

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

October 4, 2023

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

RE: Draft Amendments for COMAR 10.25.07 and 10.25.18

Dear Mr. Steffen:

Kaiser Permanente appreciates the opportunity to comment on MHCC's draft amendments to implement Chapters 248 and 249 of the Acts of 2023. 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.

In 2004, Kaiser Permanente launched the largest electronic health records system in the nation, which connects information for all our members across all our medical offices and hospitals. Clinicians have access to all Kaiser Permanente medical data for every member, enabling care teams to identify opportunities to improve the safety and quality of care. KP tracks and maintains records over decades, enabling a long-term perspective on each individual's health over time.

Our care teams also can make well-informed decisions based on a full range of patient information and can easily connect with each other to work effectively as a team. We believe that this approach is part of the reason we lead the nation in quality ratings and why research shows Kaiser Permanente members live six years longer than the national average.

Unfortunately, few health care providers have access to a comprehensive EHR that contains all of a patient's medical information and communicates care gaps and potential medical errors before they happen. As difficult and expensive as it is to integrate this kind of system across a community, it is our view that doing so is the best way to maximize quality of care for all patients.

Kaiser Permanente supports the objective of this legislation and its implementing regulations, to protect the privacy of our patients who receive legally protected health care. At the same time,

[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.

we have experienced the value of a comprehensive EHR and want to make sure that all of our members can choose to participate in that as fully as possible. To that end, we offer the following amendments. We have coordinated these amendments with several other health systems, which we hope will streamline the review process for you.

Scope

We propose clarifying that the scope of legally protected health information, defined in COMAR 10.25.18.02(B)(4) is abortion care and sensitive health services provided in Maryland after June 24, 2022, when the U.S Supreme Court issued its opinion in *Dobbs v. Jackson Women's Health Organization*. We also propose clarifying that mifepristone is in scope if prescribed for the purpose of "medical or surgical termination of pregnancy" (since it has other clinical applications), and that legally protected health information does not include e-prescribing. Finally, we propose clarifying that the diagnosis, procedure, medication, and other codes are documented in structured data fields:

(40) (a) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including:

(1) Mifepristone data, as defined by the Secretary, prescribed after June 24, 2022 to a patient located in the state of Maryland related to the diagnosis of medical or surgical termination of pregnancy; and

(2) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes documented in structured data fields related to:

(i) Abortion care provided in the state of Maryland after June 24, 2022; and

(ii) Sensitive health services provided in the state of Maryland after June 24, 2022, as defined by Health-General, §4-301, Annotated Code of Maryland.

(b) "Legally protected health information" does not include an electronic prescription and prescription related information transmitted to a pharmacy of the patient's choice.

Consent

- Health-General § 4-302.5(b)(2) permits disclosure of legally protected health information through an HIE to "a specific treating provider at the written request of and with the consent of "a patient or the patient's parent or guardian. We propose adding a definition of "specific treating provider" in COMAR 10.25.18.02:

  "Specific treating provider" means a health care provider that a patient, or parent or guardian of a patient, gives consent to receive sensitive health information in accordance with COMAR 10.25.18.04.

- We also propose clarifying in COMAR 10.25.18.04A that a patient may specify any health care provider (present or future) receive sensitive health information, even if a provider-patient relationship does not yet exist, and that consent is open-ended and may be revoked:

(2) If federal or State law requires written consent or authorization for access, use, or disclosure of sensitive health information, a person shall obtain consent or authorization consistent with the applicable law prior to the access, use, or disclosure of sensitive health information to and through an HIE to an authorized recipient*, including as follows:*

(a) A patient, or parent or guardian of a patient, providing written consent to a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may specify:

(i) Any health care provider to receive sensitive health information, at present or in the future, notwithstanding the existence of a current provider-patient relationship; and

(ii) The duration of the consent, up to and including an unlimited period of time.

(b) The consent obtained by a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may be revoked by the patient, or parent or guardian of a patient, at any time, upon reasonable notice.

- COMAR 10.25.18.03A enumerates rights of a health care consumer concerning information accessed, used, or disclosed through an HIE. We propose adding an additional right to give written consent in advance to disclosure of legally protected health information to any health care providers with home the patient may have a future relationship:

(5) The right to control sensitive health information, including the right to give written consent in advance to disclosure of legally protected health information to one or more health care providers with whom the health care consumer may have a future provider-patient relationship.

Emergency Exception

It is important for health care providers to have access to patients' medical records in an emergency when the patient is not able to provide consent or when delaying access to information could jeopardize patient health. We request that MHCC retain the emergency exception in COMAR 10.25.18.04, and propose a revision as follows:

(3) Notwithstanding §A(2) of this regulation, an HIE may transmit sensitive health information, *in accordance with state and federal law, including 42 CFR § 2.51 and Health-General Article Title 4, Subtitle 3, Annotated Code of Maryland. [*:

(a) To medical personnel who have a need for information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention, as permitted by Part 2; and

(b) In an emergency, if a health care provider makes a professional determination that an immediate disclosure is necessary to provide for the emergency health care needs of a patient or recipient.]

Enforcement

- We propose clarifying that a person who knowingly fails to comply with these regulations be subject to a fine imposed by MHCC under COMAR 10.25.18.09(C)(3):

  (3) (a) A person who knowingly fails to comply with this chapter shall be subject to a civil penalty imposed by the Commission not exceeding $10,000 per day ~~for each person impacted by the non-compliance~~ based on:

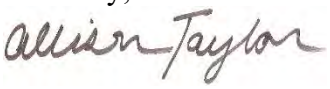
  (i) The extent of actual or potential public harm caused by the violation;
  (ii) The cost of the investigation; and
  (iii) The person's prior record of compliance.

- We also propose defining "knowingly" in COMAR 10.25.18.02 to mean actual knowledge that legally protected health information has been disclosed through an HIE in violation of state law:

  "Knowingly" means a person, at the time of making a disclosure, has actual knowledge that legally protected health information is being disclosed through an HIE and that this disclosure violates Health-General Article § 4-302.5, Annotated Code of Maryland.

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 Permanente

MEDITECH

October 3, 2023

Anna Gribble
Program Manager, Maryland Health Care Commission (MHCC)
Health Information Technology
4160 Patterson Avenue
Baltimore, MD 21215

Attention: COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses & COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Ms. Gribble,

On behalf of Medical Information Technology, Inc., (MEDITECH), I am pleased to offer comments on the *proposed amendments to COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses & COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information*.

We strongly support the feedback provided to the Maryland Health Care Commission (MHCC) on behalf of the Electronic Health Record Association (EHRA). In addition we ask that the MHCC consider the following:

For organizations who submit an implementation plan, we encourage that MHCC put specific parameters in place within the regulation detailing how soon the HIE will receive notice of the approval/denial of their plans. Any delay in this notification will impact the HIE being able to successfully develop and rollout the necessary changes by the proposed June 1, 2024 compliance date.

Additionally, we feel there are certain scenarios in which the disclosure of abortion-related data to other entities is necessary as part of the services being provided to the patient. ONC's recently proposed Health Data, Technology, and Interoperability (HTI-1) rule is similarly proposing data segmentation requirements which has received significant industry pushback given the large scope of work required to develop this functionality, lack of standards maturity for data segmentation capabilities, and major concerns around patient safety.

Given these challenges and considerations, MHCC should seek to work with industry stakeholders to advance these standardization efforts to align with those of federal agencies, as well as consider a less stringent compliance timeline to ensure the safe and successful development/deployment of these important features. Further, we recommend MHCC consider rolling out this regulation in a phased manner with the initial phase focused only on discrete data such as diagnosis codes. Phasing in these requirements will significantly reduce scope and allow HIT developers to better assess the associated challenges, opportunities, and risks.

Additionally, we request clarification and feedback on the below scenarios as to whether they fall within the scope of the regulation. Your response will assist us in determining our approach to meeting the requirements of SB 786 by the current compliance deadline.

Questions/Scenarios Seeking MHCC Feedback

- Many of the outbound HL7 interfaces that send data to other business entities and/or treating providers do so as part of the services being provided to the patient during that visit. For example, a site sends their labs outbound to a reference lab to result prenatal genetic screening tests, the results of which may determine decisions related to abortion care. What are the expectations of sending this data?

- Some organizations may have an outbound order interface which would include the sending/receipt of ultrasounds, the results of which are needed for care being provided. What are the expectations of sending this data?

These are just a few scenarios that we have discussed internally where the data being sent outbound is necessary to complete the care being provided, which in turn is in some manner related to the abortion visit.

Finally, CMS mandates the sending of Admission, Discharge, Transfer (ADT) notifications to treating providers, would the expectation be that these are suppressed for abortion-related visits per the requirements of SB 786?

We appreciate any guidance MHCC can provide so we can ensure we are providing our customers in Maryland with the best possible solution to meet these requirements.

GALLAGHER
GALLAGHER EVELIUS & JONES
ATTORNEYS AT LAW

October 4, 2023

VIA EMAIL AND U.S. MAIL

Ben Steffen
Executive Director
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215
ben.steffen@maryland.gov
mhcc_regs.comment@maryland.gov

Re: Informal Comments Submitted on behalf of Mercy Health Services to Proposed Emergency Regulations: COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information and COMAR 10.25.07, Certification of Electronic Health Networks and MedicalCare Electronic Claims Clearinghouses

Dear Mr. Steffen:

On behalf of Mercy Health Services, Inc. ("Mercy"), we write to provide informal comments to the Maryland Health Care Commission ("MHCC")'s proposed amendments to COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information and COMAR 10.25.07, Certification of Electronic Health Networks and MedicalCare Electronic Claims Clearinghouses (the "Proposed Regulations") to implement Maryland Senate Bill 786, Health – Reproductive Health Services – Protected Information and Insurance Requirements (the "Act").

Mercy appreciates the opportunity to provide informal comments and urges the MHCC to adopt the Proposed Regulations with the modifications discussed below.

I. General Comments and Policy Considerations

Mercy is an integrated health care delivery system that provides a broad array of health services throughout the State of Maryland, including at Mercy Medical Center, an acute care hospital located in downtown Baltimore. As a Catholic institution, Mercy does not provide abortion care services. It is, however, the largest birthing hospital in Baltimore City, and provides emergency services. The Act and the Proposed Regulations are therefore likely to affect Mercy patients who have received or will receive legally protected health care services and Mercy's delivery of health care services.

#852423
000342-0267

Mercy supports the important goals of the Act and the Proposed Regulations – to protect the confidentiality of patients and the special relationship of trust between providers and patients. At the same time, Mercy shares the concerns of other health care providers in the state that the Act and Proposed Regulations, as drafted, may have unintended consequences for patient care delivery.

A. The Advancement of Health IT and Interoperability and Its Impact on Care Delivery

In recent years, the federal government has focused heavily on the development of health information technology that promotes the seamless exchange of health information. The Centers for Medicare & Medicaid Services has robust electronic health record ("EHR") incentive programs to promote meaningful use of certified electronic health record technology. Through the 21st Century Cures Act, the federal government has also sought to advance interoperability, prohibit information blocking, and enhance the accessibility of electronic health information. Pub. L. No. 114-225 (2016). These initiatives all aim to make health care information more easily accessible to improve treatment and care continuity for patients. Due to these initiatives, health care providers have widely invested in EHR systems. Health information technology and EHR systems have rapidly evolved, and it is now the status quo for providers to use health information exchanges ("HIEs") to facilitate the exchange health information with other treating providers.

The use of HIEs advances patient safety and quality of care. For example, when a patient arrives at a hospital, the hospital can pull the patient's health history and medication information in real-time through the HIE, making it easier to diagnose and promptly treat the patient. In such circumstances, emergency physicians are able to view a patient's medication list and avoid a potentially dangerous medication interaction. Emergency physicians are also able to avoid unnecessary delays in obtaining patient information from other treating providers by accessing the information through the HIE. The efficient and timely exchange of health information through HIEs thus offers numerous benefits to providers and patients alike.

B. Technical Limitations of HIEs and Resulting Implementation Challenges

Based on current technical limitations of HIEs, Mercy has some concern that the Proposed Regulations may hinder progress made toward improved accessibility and seamless exchange of health information, and could have unintended consequences for patient care. The Proposed Regulations call upon HIEs to restrict the disclosure of a specific subset of treatment information related to legally protected health care. Although health information technology has progressed significantly in recent years, limitations still exist. For example, some HIEs lack the technological capabilities to support the isolated selection and restriction of *only* legally protected health information within the EHR (known as data segmentation), especially within free-text, unstructured data fields used to document patient encounters such as medical history and clinical notes. Even if this functionality did exist, there are substantial risks to data segmentation. Providers need a full and complete medical record to effectively treat their patients, and with data segmentation in use, providers may not be aware that they are missing critical information. Epic

detailed some of the key issues related to data segmentation in its comments to the Office of National Coordinator's 2020 proposed regulations regarding health data, technology, and interoperability, an excerpt of which is attached as **Exhibit A**.

Given the limitations of existing technology, it may not be possible to restrict *only* a patient's legally protected health information from disclosure through an HIE while keeping the remainder of the patient's record available. As a result, in order to comply with the law, patients who have received legally protected health care may need to be opted out completely from participating in an HIE, meaning that no portion of their records will be accessible. This has the potential to negatively impact care for these patients, especially in emergency situations, when prompt access to a patient's treatment records is critical. This may also interfere with a consumer's right to control access and exchange of their health information through an HIE, which is recognized under the MHCC's Existing Regulations.

To implement the Proposed Regulations, HIEs and providers will likely need to alter the status quo for how health care is documented within the EHR. Documentation of legally protected health care services may currently be reflected in a multitude of fields within an electronic health record (i.e., medications list, history, clinical notes). Going forward, providers will need adopt new protocols for documenting such care in order to comply with the Act's disclosure restrictions, such as developing "sensitive" clinical note templates to identify encounters that involve legally protected health care and ensure they are not released through an HIE. HIEs may also need to modify their available functionality to adequately restrict disclosure of legally protected information.

In addition, providers will likely need to alter policies for how consent will be obtained from patients to disclose their health information through an HIE. The Act and Proposed Regulations permit disclosure of legally protected health information through an HIE with written consent. Some HIEs only offer organization-wide patient consent processes, meaning the provider has a binary option to require consent from all or no patients. Therefore, providers may be required to obtain consent from all patients, which may create new workflow challenges and delays.

C. Proposed Comments Aim to Align with MHCC Principles of Improved Access to Records and Honoring Consumer Choice

The MHCC's Existing Regulations recognize the benefits and importance of HIEs in advancing safe and effective patient care. Pursuant to Maryland Code, Health-General Article, § 4-302.3(j), the MHCC is charged with adopting regulations regarding the exchange of clinical information through HIEs to "improve treatment, including improved access to clinical records by treating clinicians." MHCC expressly recognizes that a core purpose of its HIE regulations is "to improve access to clinical records by treating clinicians." COMAR 10.25.18.01A(3).

Keeping the above principles in mind, Mercy has suggested changes to the Proposed Regulations to maintain consistency with applicable law, MHCC's statutory charge of improving access to clinical records by treating providers, and the Existing Regulations' focus on honoring a consumer's choice regarding access to their health information through an HIE.

II. Comments on Specific Proposed Regulations: COMAR 10.25.18

A. Scope

It is essential to clarify the scope of the regulations so HIEs and health care providers understand the scope of care documentation and operations covered by these regulations.

1. Legally Protected Health Information – Regulation .02

The Proposed Regulations require restrictions on disclosure of legally protected health information through an HIE. The Act does not address whether it applies only to legally protected health care provided on or after its effective date, or whether it is intended to apply to legally protected health care provided prior to its effective date. On June 24, 2022, the U.S Supreme Court issued its opinion in *Dobbs v. Jackson Women's Health Organization,* No. 19-1392, 597 U.S. ___ (2022*),* overturning *Roe v. Wade* (1973) and concluding that the U.S. Constitution does not protect the right to an abortion. In advance of this decision, many states passed "trigger laws" restricting or banning abortions altogether that would take effect immediately in the event the Supreme Court overturned *Roe v. Wade*. The U.S. Constitution prohibits states from passing ex post facto laws, which are laws that impose criminal liability for an act previously committed that was innocent when done. U.S. Const. art. I, § 10, cl. 1. This means abortion care services retained legal protection consistent with *Roe v. Wade* precedent until June 24, 2022 and individuals are likely to be shielded from prosecution for abortion services received prior to that date.

Providers' EHR software does not have the current technical capability to search, identify, and restrict legally protected health care services documented in unstructured (i.e., free-text) fields within the EHR. Given the current technical limitations of HIEs, it will be difficult, if not impossible, for providers to identify all references to legally protected health information within existing records, which could include patient care encounters dating back five to ten years or more. Because abortion care services were protected consistent with *Roe v. Wade* in all states until June 24, 2022, Mercy proposes that MHCC's regulations apply only to legally protected health care provided on or after June 24, 2022. This clarification will serve the Act's aim of protecting patients and providers from prosecution for seeking or providing legally protected health care, while reducing the administrative challenges for providers of identifying legally protected health information in existing records.

The Act states that an HIE or EHN "may not disclose *mifepristone data or the diagnosis, procedure, medication, or related codes* for abortion care and other sensitive health services as

determined by the Secretary under subsection (D)[.]" Md. Code, Health-General § 4-302.5(B) (emphasis added). Similarly, subsection (D)(3)(I) provides the "Secretary shall adopt regulations to restrict the disclosure of abortion care and other sensitive health services information by *diagnosis, procedure, medication, or related codes*[.]" Thus, the Act is focused on restriction of specific and structured data fields – diagnosis, procedure, and medications – or their related codes as determined by the Secretary. Mercy therefore proposes the definition of "legally protected health care" should be limited to data documented in these structured data fields as enumerated in the Statute and by the Secretary.

Additionally, Mercy notes that while Mifepristone is commonly used for medical termination of a pregnancy, Mifepristone has other clinical indications unrelated to abortion care. For example, Mifepristone may be prescribed to treat tumors on the uterine wall, Cushing's syndrome, and for miscarriage management. Mercy proposes to clarify that the restrictions on disclosure set forth in the Proposed Regulations relate only to the prescription of Mifepristone for abortion care, consistent with the intent of the Act.

Finally, given that MHCC regulates HIEs' operations within Maryland, Mercy proposes that the Proposed Regulations define legally protected health information as related to legally protected health care provided in Maryland. Md. Code, Health-General § 4-302.2(b)(1).

Mercy proposes the following amendments to the definition of "legally protected health information" to incorporate the foregoing considerations as to the appropriate scope of the Proposed Regulations:

"(40) (a) 'Legally protected health information' means the health information subject to restrictions under Health-General Article, § 4-302.5, Annotated Code of Maryland, including:

(1) Mifepristone data, as defined by the Secretary, prescribed after June 24, 2022 to a patient located in the state of Maryland related to the diagnosis of medical termination of pregnancy; and

(2) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes documented in structured data fields related to:

(i) Abortion care provided in the state of Maryland after June 24, 2022; and

(ii) Sensitive health services provided in the state of Maryland after June 24, 2022, as defined by Health-General, §4-301, Annotated Code of Maryland.

(b) "Legally protected health information" does not include an electronic prescription and prescription related information transmitted to a pharmacy of the patient's choice."

2. Exclusions - Regulation .01

The Proposed Regulations exclude from coverage insurance carriers and their business associates. Mercy proposes the same exclusion should apply with respect to health care providers and their business associates, since these are similarly situated parties with special obligations governed by HIPAA. The Proposed Regulations also provide an exclusion for hospitals and their ancillary clinical service providers. Mercy suggests this exclusion be modified to apply not only to hospitals, but also to other types of health care provider organizations (i.e., nursing homes or ambulatory surgical facilities) who may have ancillary clinical service providers that are similarly situated to hospital ancillary providers. Mercy proposes the following changes to Proposed Regulation .01C:

"C. This chapter does not apply to:

(1) Protected health information exchanged, accessed, used, or disclosed . . .

(c) Between a ~~hospital~~ health care provider and its affiliated ancillary clinical service provider who is affiliated with the ~~hospital~~ health care provider and who, if required by HIPAA, has entered into a business associate agreement with the ~~hospital~~ health care provider.

. . .

(g) Between a health care provider and its business associate, as defined in 45 C.F.R. § 160.103."

B. Exception for Disclosure in Emergency Circumstances – Regulation .04

It is critical that providers have access to patients' medical information in an emergency when the patient may be incapable of providing consent or when delaying access to such information could jeopardize the patient's health. Emergency department clinicians rely on HIEs to provide essential information about a patient's medications and health history in order to properly diagnose and treat the patient.

Due to the technical limitations described in Section I.B above, hospitals and other providers may be required to adopt policies and procedures requiring that written consent be obtained from patients[1] before releasing any of their health information through an HIE. A consent process is not feasible where the patient is unconscious or in need of immediate care, when delaying care to obtain signed, written consent could compromise the patient's health.

Under HIPAA and the Maryland Confidentiality of Medical Records Act ("MCMRA"), health care providers are permitted to disclose health information to another health care provider for treatment purposes without needing to obtain written patient consent or authorization, including in an emergency circumstance. 45 C.F.R. § 164.506(c)(2); Md. Code, Health-General § 4-305(b)(4). The MCMRA also permits disclosure of medical records without the need for written patient authorization, "[i]f a health care provider makes a professional determination that an immediate disclosure is necessary, to provide for the emergency health care needs of a patient or recipient." Md. Code, Health-General § 4-305(b)(6). Unlike HIPAA and MCMRA, the 42 C.F.R. Part 2 ("Part 2") Regulations require patient consent for disclosure of Part 2 information for treatment purposes, due to the special privacy concerns of that information. However, even the Part 2 Regulations provide an exception for disclosure in medical emergencies, stating "patient identifying information may be disclosed to medical personnel to the extent necessary to . . . meet a bona fide medical emergency in which the patient's prior written consent cannot be obtained" and permit disclosure if a patient's consent cannot be obtained because the Part 2 provider is closed during a state of emergency. 42 C.F.R. § 2.51(a). Accordingly, it would be consistent with HIPAA, the MCMRA, and the Part 2 Regulations, to recognize an exception for disclosure of sensitive health information through an HIE in emergency circumstances without requiring patient consent.

[1] Providers are still evaluating whether the technical capabilities available through HIEs will enable them to obtain written consent from only those patients who have received legally protected health care, or if they will be presented with a binary option to obtain consent from all patients or none, in which case they will need to obtain consent from all.

The Act does not address emergency disclosures, and MHCC has been given the authority to adopt HIE regulations "specify[ing] the scope of clinical information to be exchanged" and "restrict[ing] data of patients who have obtained legally protected health care." Md. Code, Health-General § 4-302.3(j)(1)(i), (j)(3)(iv). It is within MHCC's purview to address and clarify when emergency disclosures of legally protected health information are permitted under its Proposed Regulations. *See, e.g., J.H. v. Prince George's Hospital Center*, 233 Md. App. 549 (2017) (in adopting regulations to implement a statute that failed to address a certain issue, the Maryland Department of Health permissibly passed a regulation that "fill[ed] in the gap left by the statute."); *Bd. Of Liquor License Com'rs for Balt. City v. Hollywood Productions*, 344 Md. 2, 11 (1996) (In cases where the Legislature has broadly delegated authority to an administrative agency, the scope of the agency's implied authority to regulate in that area is "quite liberally construed.").

It is imperative that MHCC retain an emergency exception within Proposed Regulation .04 to ensure patients' critical information is available through an HIE in an emergency. Mercy proposes that the following emergency exception replace the language within Proposed Regulation .04A(3):

"(3) Notwithstanding §A(2) of this regulation, an HIE may transmit sensitive health information in accordance with state and federal law, including 42 CFR § 2.51 and Health-General, Article Title 4, Subtitle 3, Annotated Code of Maryland.

~~If federal or State law does not require written consent or authorization for access, use, or disclosure of sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE.~~"

Due to current technical limitations as described in Section I.B above, providers may need to adopt a policy requiring all patients to provide written consent to exchange their health information through an HIE; in this case, federal or State law would not require such authorization from those patients who have not received legally protected health care, but technical solutions may dictate a binary all or nothing approach. As reflected above, Mercy proposes that MHCC strike the current language in Proposed Regulation .04A(3), as it may be infeasible for providers to honor the Act's consent requirements without violating this proposed provision.

C. Health Care Consumer Rights Regarding Access, use, and Disclosure of Sensitive Health Information

1. Definition of "Specific Treating Provider" – Regulation .02

Maryland Code, Health-General § 4-302.5(b)(2) permits disclosures of legally protected health information through an HIE to "a specific treating provider at the written request of and with the consent of" a patient or the patient's parent or guardian. The term "specific treating provider" is not defined in the Act or the Proposed Regulations. Mercy urges the MHCC to adopt a definition of "specific treating provider" that aligns with the consent requirements of the Part 2 Regulations. The Part 2 Regulations provide that "[a] written consent to a disclosure under the regulations in this part may be paper or electronic and must include … [t]he name(s) of the individual(s) *or the name(s) of the entity(-ies)* to which a disclosure is to be made." 42 C.F.R. § 2.31 (emphasis added). Consistent with the Part 2 Regulations, patients should have the ability to consent to disclosures of legally protected health information to entities in addition to particular clinicians, at the patient's option. Such a definition promotes patient autonomy over their legally protected health information and recognizes that patients may wish to consent to disclosure of their information on an organization-wide basis to improve efficiency and effectiveness of the patient's health care. Mercy proposes to add a definition of "specific treating provider" as follows:

"(#) 'Specific treating provider' means a health care provider to which a patient, or parent or guardian of a patient, gives consent to receive sensitive health information in accordance with COMAR 10.25.18.04."

2. Consent to Disclosure of Sensitive Health Information – Regulation .04

In addition to defining the term "specific treating provider," Mercy proposes that the MHCC amend Proposed Regulation .04 to provide additional clarity to providers, patients, and HIEs as to the consent requirements for the disclosure of sensitive health information. One primary purpose of the MHCC's Existing Regulations is to provide health care consumers with control and choice over how their health information is exchanged. Consistent with this focus, Mercy proposes the following amendments to Proposed Regulation .04A(2), which will clarify that patients may provide consent to the disclosure of their sensitive health information on a prospective basis if desired and to revoke consent at any time:

"(2) If federal or State law requires written consent or authorization for access, use, or disclosure of sensitive health information, a person shall obtain consent or authorization consistent with the applicable law prior to the access, use, or

disclosure of sensitive health information to and through an HIE to an authorized recipient, including as follows:

(a) A patient, or parent or guardian of a patient, providing written consent to a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may specify:

(i) Any health care provider to receive sensitive health information, at present or in the future, notwithstanding the existence of a current provider-patient relationship; and

(ii) The duration of the consent, up to and including an unlimited period of time.

(b) The consent obtained by a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may be revoked by the patient, or parent or guardian of a patient, at any time, upon reasonable notice."

3. Consumer Right to Make Educated Decision Regarding Participation in an HIE – Regulation .03A

The Existing Regulations recognize the importance of empowering health care consumers to control access to their health information through an HIE. MHCC's Existing Regulations give health care consumers the right to be educated on "the risks and benefits of participating in [an] HIE" and to make their own decisions about what level of participation best serves their needs. COMAR 10.025.18.03A(1)(b). As drafted, the Proposed Regulations have the effect of limiting consumer autonomy and choice as it relates to their participation in an HIE. Patients should have the flexibility to consent to disclosure of their sensitive health information to any subset of health care providers, including on a prospective basis. This will reduce patient burden to execute numerous consent forms and will enable providers to access information more efficiently for patients who desire their information to be accessible to one or more of their treating providers. Mercy proposes to amend Proposed Regulation .03A to add a new subsection (5) as follows:

"(5) The right to control sensitive health information, including the right to give written consent in advance to disclosure of legally protected health information to one or more health care providers with whom the health care consumer may have a future provider-patient relationship."

D. Registration and Enforcement – Regulations .02 and .09

1. Definition of "knowingly" – Regulation .02

Mens rea refers to the criminal intent required to convict a person of a particular crime. The *mens rea* requirement is based on the idea that a person must possess a guilty state of mind and be aware of his or her misconduct to commit a crime. The term "knowingly" does not have a uniform definition or meaning, and is not currently defined by the Act or Proposed Regulations. Given the significant repercussions for a violation of the Act or the Proposed Regulations – to be charged with commission of a crime and penalties of up to $10,000 per day – MHCC must adopt a definition of "knowingly" to give adequate notice of the intent required to result in a criminal or civil violation subject to penalties under COMAR 10.25.18.09C(3). Maryland Code, Health-General § 4-302.5C(1) states that a person may be convicted of a misdemeanor if the person "*knowingly violates* [Health-General Article, Section 4-302.5]." Thus, knowingly modifies *violates the law*, meaning a person must be aware that their conduct violates the law. Similarly, the Proposed Regulations provide that a person "who *knowingly* fails to comply with this chapter shall be subject to a civil penalty not exceeding $10,000 per day[.]" Proposed Regulation .09C(3)(a) (emphasis added). Mercy proposes the MHCC adopt the following definition of the term "knowingly":

"(#) 'Knowingly' means a person, at the time of making a disclosure, has actual knowledge that legally protected health information is being disclosed through an HIE and that this disclosure violates Health-General Article § 4-302.5, Annotated Code of Maryland."

2. Clarifications Regarding Civil and Criminal Penalties – Regulation .09

Maryland Code, Health-General § 4-302.2(b)(iv) states that MHCC may "[p]rovide appropriate penalties for noncompliance with its HIE regulations, including fines that do not exceed $10,000 per day" based on specified factors. Accordingly, Mercy suggests MHCC revise

its proposed civil penalties provision to reflect a maximum of $10,000 per day as reflected in the Code, rather than "10,000 per day *for each person impacted by the non-compliance*," which implies penalties could be applied in excess of $10,000 per day. Mercy also proposes MHCC clarify that the civil penalties may be imposed only by the MHCC and there is no private right of action available under its Proposed Regulations. Finally, Mercy suggests MHCC clarify the date on which its civil penalties will become effective, which should be no earlier than the effective date of its final regulations.

The Act calls for penalties to be assessed based on specific factors set forth under Maryland Code, Health-General § 4-302.5(c)(2), including the final factor, "whether the person previously violated this section." The Proposed Regulations should clarify that an assessment of a person's prior record of compliance relates to its compliance with Maryland Code, Health-General § 4-302.5, rather than broad inquiry into its compliance history with any laws.

In light of these comments, Mercy suggests the following changes to Proposed Regulation .09C(3):

"(a) Civil penalties. Beginning on the effective date of this section, ~~A~~ a person who knowingly fails to comply with this chapter shall be subject to a civil penalty imposed by the Commission not exceeding $10,000 per day ~~for each person impacted by the non-compliance~~ based on:

(i) The extent of actual or potential public harm caused by the violation;

(ii) The cost of the investigation; and

(iii) The person's prior record of compliance.

(b) Criminal penalties. Beginning June 1, 2024, a person who knowingly violates Health-General Article, §4-302.5, Annotated Code of Maryland, shall be guilty of a misdemeanor and on conviction is subject to a fine not to exceed $10,000 per day based on:

(i) The extent of actual or potential public harm caused by the violation;

(ii) The cost of the investigation; and

(iii) The person's prior record of compliance with Health-General Article, §4-302.5, Annotated Code of Maryland."

E. Suspension of HIE Registration – Regulation .05C

The Existing Regulations allow the MHCC to suspend the registration of an HIE in response to a single unauthorized disclosure. HIEs are subject to stringent privacy and security requirements and must take steps to safeguard the information they exchange. As discussed throughout these comments, HIEs play a vital role in the efficient and effective delivery of health care. Consistent with other state and federal laws governing the privacy and security of electronic health information, Mercy recommends that the MHCC take action to suspend an HIE only when the HIE has demonstrated a pattern or practice of inappropriate disclosures. This recognizes that interruptions to HIE connectivity should be limited where possible to facilitate the access and exchange of information necessary for high quality care, while protecting the security and integrity of the information that is exchanged. Mercy proposes the following amendments to Proposed Regulation .05C:

"The Commission may suspend the registration, in accordance with Regulation .09 of this chapter, of a registered HIE that engages in a pattern or practice of inappropriately ~~discloses~~ disclosing to any person any PHI, or health information derived from PHI, that is available through the HIE's infrastructure, except as consistent with or otherwise permitted by this chapter and applicable federal or State law."

F. Requirements for Accessing, Using, or Disclosing of Data Through an HIE for Secondary Use – Regulation .10

While the Proposed Regulations allow secondary use of sensitive health information when permitted by state or federal law, Mercy recommends that the Proposed Regulations expressly permit the use of de-identified data and limited data sets that include sensitive health information for secondary use. Such a provision does not conflict with the Act and would offer several practical benefits. The MHCC is required to submit quarterly reports on the implementation of the Act in fiscal years 2024 and 2025. The effects of the Act will also need to be studied in the future to evaluate the impact to patient care. These reports and studies may necessarily require access to sensitive health information in a limited data set or in de-identified form. Both HIPAA and 45 CFR Part 46, Subpart A (the "Common Rule") recognize that limited data sets and de-identified data

have important uses in research activities, which further supports the adoption of the provision recommended below. Moreover, sensitive health information may be relevant to legitimate population health management and research activities. The Existing Regulations already provide sufficient safeguards for secondary use of data for population health management and research purposes, and it would be detrimental to exclude sensitive health information categorically from such activities. Mercy proposes the following amendment to Proposed Regulation .10:

"A. An HIE shall not use or disclose a patient's identifiable sensitive health information for secondary use unless permitted by applicable federal or State laws and regulations. An HIE may disclose a patient's sensitive health information that has been de-identified or as part of a limited data set in accordance with 45 C.F.R. § 164.514 for secondary use in accordance with Sections B and C of this Regulation."

G. Right to Judicial Review of Final Decision – Regulation .09

The Proposed Regulations should clarify that a final decision of the MHCC related to an enforcement action, following the hearing process set forth at Regulation .09D or the exceptions process set forth at Regulation .09E, is subject to judicial review by an aggrieved party in accordance with the Maryland Administrative Procedure Act. Mercy proposes the following modifications to Proposed Regulation .09 to add a new subsection F following Regulation .09E and to re-letter the section following .09F as .09G and .09H:

"F. Final Decision and Judicial Review.

(1) The Commission shall issue a final decision on the enforcement action following a hearing under Regulation .09D or the exceptions process under Regulation .09E of this Chapter based on the record of the proceeding.

(2) The final decision shall be in writing and state the reasons and grounds for the Commission's decision.

(3) The Commission's final decision is subject to judicial review in accordance with the Maryland Administrative Procedure Act, State Government Article, Title 10, Annotated Code of Maryland.

(4) In order to take a judicial appeal, a person must be an aggrieved party."

Mercy also suggests the MHCC specify in its Proposed Regulations which records are part of the record of the proceedings for purposes of judicial review. Finally, Mercy proposes the MHCC add a definition of aggrieved party to Proposed Regulation .02B:

"(#) 'Aggrieved party' is a person who is the subject to the enforcement action and would be adversely affected by the final decision of the Commission, or the Secretary."

III. Comments on Specific Proposed Regulations: COMAR 10.25.07

A. Definition of "Adjudication of Claims" – Regulation .02

Maryland Code, Health-General § 4-302.5(b)(2) permits disclosures of legally protected health care information through an HIE "for the adjudication of claims." The term "adjudication of claims" is not defined in the Act or the Proposed Regulations. To provide clarity to EHNs and participating organizations, Mercy proposes to include a definition of "adjudication of claims" as follows:

"(#) 'Adjudication of claims' means the activities taken by a health care provider, payor, or health plan related to the past, present, or future payment for the provision of health care to an individual."

* * *

Mercy appreciates the opportunity to comment on these Proposed Regulations. Mercy supports the goals of the MHCC and of the Legislature to protect patient privacy and safeguard

the patient-provider relationship. Mercy also supports the continued advancement and modernization of health information exchange and encourages the MHCC to adopt final regulations that balance these important policy aims.

Thank you for your consideration of these comments. Please contact us if you have any questions.

Very truly yours,

Mallory Regenbogen

Mallory Regenbogen

Alison Lutich

Gallagher Evelius & Jones LLP
218 N. Charles Street, Suite 400
Baltimore, MD 21201

cc by email:

David Sharp, Director, Center for Health Information Technology and Innovative Care Delivery, MHCC
Anna Gribble, Program Manager, Center for Health Information Technology and Innovative Care Delivery, MHCC
Alexa Bertinelli, Esq., Assistant Attorney General, MHCC
Caitlin E. Tepe, Esq., Assistant Attorney General, MHCC
Ruby Potter, Health Facilities Coordinator, MHCC
Ryan O'Doherty, Senior Vice President, External Affairs, Mercy
Claudine Schiro-Baker, Senior Vice President and Chief Information Officer, Mercy

EXHIBIT A

June 20, 2023

Submitted electronically

Micky Tripathi, Ph.D., M.P.P.
National Coordinator for Health Information Technology
Office of the National Coordinator for Health Information Technology
U.S. Department of Health and Human Services
330 C St SW, Floor 7
Washington, DC 20201

Re: Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing (RIN 0955-AA03)

Dear Dr. Tripathi:

Thank you for the opportunity to provide comments on ONC's proposed updates to the certification program and information blocking requirements. We appreciate ONC's recognition of the important role TEFCA can play in advancing information sharing and use of a clear and transparent process in proposing updates to USCDI. Although we support many of ONC's goals, key aspects of the proposed rule relating to information blocking, patient-requested restrictions, and predictive DSI should be adjusted. In particular, the proposed requirement that EHRs have functionality to hide data from clinicians through data silos takes a major step backward in advancing patient care and health information exchange.

Our full comments are attached. Below, we highlight significant adjustments ONC should make:

Information blocking enhancements

As the industry leader in interoperability, Epic has long supported ONC's goal to advance health information sharing. Our interoperability platform, Care Everywhere, is responsible for 12.7 million record exchanges every day (slightly less than half are with other vendors' EHRs). We were a founder of Carequality, a national health information exchange framework, and we provide more FHIR resources than any other certified EHR developer. Recently, Epic TEFCA Interoperability Services was approved to onboard as a Qualified Health Information Network (QHIN) under TEFCA. So far, more than 40 of our major health system customers have pledged to join TEFCA. These customers span 37 states and include more than 250 hospitals and 8,200 clinics.

ONC's original rule implementing the 21st Century Cures Act was intended to discourage information blocking rather than encourage organizations to share data. We have long encouraged ONC to create a clear roadmap that provides regulatory certainty on how regulated actors can be good information sharers and avoid information blocking. ONC's proposal to align TEFCA and information blocking is a step in the right direction. ONC should take one step further to encourage participation in TEFCA. Specifically, ONC's proposal should be strengthened by adjusting the proposed TEFCA Condition exception to information blocking to place a burden on *any requester*—regardless of whether they are currently a TEFCA QHIN, participant, or sub-participant—to explain why joining TEFCA is infeasible or poses an undue burden for their request.

We support ONC's proposed new Infeasibility Exception condition for Third Party Modification of EHI and appreciate ONC's recognition of the risk posed by unauthorized modification of electronic health information, as well as the burden imposed should the infeasibility exception have to be used in every case. In addition, ONC should improve the definition of "offer," clarify the Manner Exception, and make improvements to the Infeasibility Exception.

§ 170.315(d)(14) - Patient Requested Restrictions Certification Criterion

Included in Base EHR Definition? **No**

(d)* * *

(14) Patient requested restrictions.

(i) For any data expressed in the standards in § 170.213, enable a user to flag whether such data needs to be restricted from being subsequently used or disclosed as set forth in 45 CFR § 164.522; and

(ii) Prevent any data flagged pursuant to paragraph (d)(14)(i) of this section from being included in a use or disclosure.

Preamble FR Citation: **88 FR 23821** Specific questions in preamble? **Yes**

Regulatory Impact Analysis: **Please see 88 FR 23898 for estimates related to this proposal.**

ONC's proposal to require data segmentation tools to support patient-requested restrictions on uses and disclosures of their HIPAA-protected health information puts patients at considerable risk of not receiving safe and effective care. The proposal takes big steps backward with regard to efforts to empower physicians with useful and comprehensive data about their patients, improve coordination across the various departments of healthcare organizations, and expand interoperability throughout care settings. In making this proposal, ONC ignores technical, clinical, and policy issues with data segmentation that have been understood for decades. It will lead to steps backward on improvements made over time. Our comments respond to the proposed certification requirements in 170.315(d)(14) and the updates to 170.315(e)(1), as well as to the health IT capabilities for data segmentation and user/patient access RFI in the notice of proposed rulemaking.

EHRs must be sources of truth for healthcare providers

Data segmentation results in withholding relevant clinical data from certain providers, undermining the EHR as a source of accurate information. Government and industry experts widely agree that timely access to accurate and complete EHRs is a powerful tool in helping patients receive correct diagnoses and high-quality care:

- When comparing the relative contributions of medical history, physical examination, and laboratory investigation to a medical diagnosis, a groundbreaking study determined that the **medical history was the key contributor to the diagnosis 76% of the time**.[3]

[3] Contributions of the History, Physical Examination and Laboratory Investigation in Making Medical Diagnoses, Peters, Holbrook, De Von Hales, Smith, and Staker.

- In the Institute of Medicine's seminal study on medical errors, *To Err is Human*, "**timely access to accurate and complete patient information"** was listed as an important component to ensuring appropriate medication use.[4]
- The U.S. Department of Health and Human Services (HHS) and its agencies routinely emphasize the connection between the provider's access to complete and accurate health information and high-quality care. As an example, ONC's current website says, "**When health care providers have access to complete and accurate information, patients receive better medical care**."[5]
- ONC's current website states, "**With EHRs, providers can have reliable access to a patient's complete health information**. This comprehensive picture can help providers diagnose patients' problems sooner."[6]

ONC's proposal ignores well-known data segmentation risks

ONC has long understood the challenges with data segmentation. In 2010, ONC commissioned a review of policy considerations related to data segmentation. The report of the review was authored by Melissa Goldstein, JD, an associate professor at the George Washington University Medical Center, and Alison Rein, MS, a director at Academy Health.[7] The report raised important technical considerations and recommended ONC study and address them. Specifically:

- The report discussed provider documentation practices in free-text fields resulting in unstructured data that can "complicate segmentation, which relies on the documentation of information in a structured and codified manner than can be managed through the application of rules engines and other intelligence systems."[8]
- The report summarized consumer engagement and provider reluctance issues. From a provider perspective, the report noted the reliance of physicians on the "availability of accurate and relevant health information in order to provide appropriate and high-quality care." The authors stated that segmentation policies "must address" provider concerns on how segmentation would impact the "quality and safety of the care provided, workflow implications, and liability."[9]

Also in 2010, the National Committee on Vital and Health Statistics (NCVHS) recommended steps HHS should take to evaluate data segmentation.[10] The committee recommended using specified categories of sensitive health information as a "basis for research, technical development, pilot testing, and

[4] To Err is Human, IOM, Page 37.
[5] Improved Diagnostics & Patient Outcomes | HealthIT.gov
[6] Id.
[7] DATA SEGMENTATION IN ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS (healthit.gov)
[8] Id at ES-2.
[9] Id.
[10] November 10, 2010 letter to HHS Secretary Kathleen Sebelius from Justine Carr, MD, Chairperson, National Committee on Vital and health Statistics. 101110lt.pdf (hhs.gov)

potential future demonstration projects. Aims of these investments should be to understand the feasibility, need for technical standards, effects on patient care, efficacy for privacy protections, benefits and costs, and other possible consequences of segmenting these categories and implementing granular patient consent for their use in particular contexts."[11]

ONC fails to reconcile how the basis for its proposal conflicts with NCVHS recommendations, the basis for other rulemakings currently proposed by other HHS agencies, and bipartisan input from members of Congress:

- HHS's Substance Abuse and Mental Health Administration's (SAMHSA) current proposed rule to adjust the Part 2 privacy regulations raises significant concerns with data segmentation. Specifically, SAMHSA says, "**The need to segment Part 2 records from other health records created data ''silos'' that hamper the integration of SUD treatment records into entities' electronic record systems** and billing processes, which in turn may impact the ability to integrate treatment for behavioral health conditions and other health conditions."[12]
- HHS's Office for Civil Rights' (OCR) current proposed rule to support reproductive healthcare privacy relies heavily on the importance of complete medical records as a basis for the proposal. In particular, OCR states, **"With complete medical records, an individual is more likely to receive appropriate ongoing or future health care, including correct diagnoses, and obtain appropriate guidance, empowering the individual in making informed treatment decisions."** OCR further states, **"[I]f an individual's medical records lack complete information about the individual's health history, a subsequent health care provider may not be able to conduct an appropriate health assessment to reach a sound diagnosis and recommend the best course of action for the individual."**[13]
- Bipartisan concerns on data segmentation have been raised by members of Congress about segmented substance use health records. U.S. Representative Earl Blumenauer (D-OR) stated, "It is a disgrace that doctors are treating patients, in the midst of the opioid crisis, without being able to obtain and understand their full medical history. **If substance use disorder treatment is not included in your entire medical records, then [such records] are not complete**."[14] U.S. Senator Markwayne Mullin (R-OK), then a member of the U.S. House, stated, "It's time that we stop stigmatizing those struggling with opioid abuse and give physicians the tools they need to help their patients. **Mental health and physical health have [each] been treated in a silo for too long**."[15]

[11] Id at P. 14
[12] Notice of Proposed Rulemaking, Confidentiality of Substance Use Disorder (SUD) Patient Records, P. 74253 of Federal Register Vol. 87, No. 231, Friday, December 2, 2022.
[13] Notice of Proposed Rulemaking, HIPAA Privacy Rule To Support Reproductive Health Care Privacy, P. 23547 of Federal Register Vol. 88, No. 73, Monday, April 17, 2023.
[14] Notice of Proposed Rulemaking, Confidentiality of Substance Use Disorder (SUD) Patient Records, P. 74221 of Federal Register Vol. 87, No. 231, Friday, December 2, 2022.
[15] Id.

Without addressing any of this information, ONC merely states there are unresolved issues, and then proceeds to propose requiring health IT developers to create segmentation tools in support of patient requests for restrictions of uses or disclosures of their protected health information in to achieve certification. Specifically, ONC states, "Patient-directed privacy of data the patient deems sensitive requires attention to specific challenges from both a technology and a policy perspective, which we recognize cannot be easily solved."[16]

ONC can succeed by focusing on a set of key patient privacy scenarios

In our commentary below, we highlight the clinical, technical, and patient trust issues with the proposed rule update and the serious risks of harm it creates for patients, care teams, and members of the general public. We conclude by recommending an approach that would allow ONC to move forward on its privacy goals in a way that is safe for patients and feasible for healthcare providers and health IT developers.

Clinical Issues

The primary clinical concern with segmentation is that treating clinicians may not have access to relevant clinical information because it is hidden. The case of Libby Zion in New York illustrates the risks to patients when clinicians do not have complete medical records. "In 1984, a college freshman named Libby Zion was admitted to the emergency room with high fever and agitation. The resident physicians administered a sedative and painkiller, not knowing that Libby was taking a contraindicated antidepressant. She died from cardiac arrest soon after. In Libby's case, her providers could not safely medicate her because they lacked access to her medical history."[17]

Restricting clinician access to relevant clinical information puts the safety of patients, care team staff, and the general public at risk. Consider just a few examples of the potential consequences of segmented data:

- A patient wants to restrict uses and disclosures of their substance use disorder information, and a provider agrees. If the patient takes buprenorphine for Opioid Use Disorder (OUD), should OUD be hidden from the patient's problem list, creating a risk of preventable harm when another physician, without this information, prescribes opioids to manage the patient's pain? Further, how does ONC reconcile its requirements in this situation with state requirements for submitting patients' medication information to Prescription Drug Monitoring Programs?

[16] Notice of Proposed Rulemaking, Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing, P. 23821 of Federal Register Vol. 88, No. 74, Tuesday, April 18, 2023.
[17] Butler, Mary. "Preventing Healthcare's Top Four Documentation Disasters" Journal of AHIMA 86, no.7 (July 2015): 18-23.

- A patient with a history of OUD wants to restrict uses and disclosures of their mental health information, including medications, and a provider agrees. Their surgeon might prescribe antidepressants or anticonvulsants off-label post-operatively as part of pain management to avoid prescribing opioids. If the patient already takes those medications to treat mental health conditions, such as a selective serotonin reuptake inhibitors (SSRI), then they may receive too high of a dose and increase their risk for serotonin syndrome.

- A patient expresses sensitivity about being on the weight-loss medication semaglutide (Wegovy, Ozempic) and wants to restrict access to and use of that information; a provider agrees. Semaglutide slows gastric emptying, meaning that food remains in the stomach longer than normal. If a surgical team doesn't know the patient takes this medication and the patient doesn't stop taking the medication appropriately prior to a surgery, the surgical team will not be aware of the patient's increased risk of aspiration while under anesthesia. As of 2022, approximately 5 million prescriptions had been issued for semaglutide.

- A patient wants to restrict users from viewing a "history of violence" reference in their problem list, and a provider agrees based on the understanding that the documented incidents occurred several years ago; the provider no longer considers the patient to pose the same risk based on their personal experiences with the patient. The patient then presents to an emergency department (ED) after a stressful situation that creates a potential for the patient to act violently again. Normally, upon arrival to the ED, the care team would see the "history of violence" reference, recognize the safety risks posed by the patient, and take precautions to protect staff and other patients and visitors. In this case, the staff are unaware. A caregiver working alone with the patient could be at serious risk for physical harm.

- A patient wants to restrict uses and disclosures of information about their history of alcohol dependency, and a provider agrees. EDs can have distinct workflows for patients with alcohol dependency due to their potential for aggression or need for ethanol or other workflows to prevent patient harm. Without the relevant information, both the patient and their care team could be at risk.

- A patient wants to restrict uses and disclosures of information that could impact an application for a job that requires a health assessment by a physician, and a provider agrees, not fully appreciating the types of jobs the patient intends to apply for. As an example, commercial airline pilots and truck drivers undergo a review for health conditions determined by the Federal Aviation Administration and the Department of Transportation to be incompatible with the safe performance of these positions. If a pilot hides a condition like epilepsy, or a truck driver hides a history of sleep apnea, a physician could not accurately assess their physical fitness for employment in roles that bear responsibility for the safety of thousands of individuals on a daily basis.

- A patient wants to restrict uses and disclosures of information related to an infectious disease diagnosis, such as a COVID-19 or Hepatitis C, and related medications, based on concern that they may be discriminated against as a result of their diagnoses; a provider agrees. If the patient were to have surgery, the care team would not be aware of infection risks for the patient and care team members, and the surgeon could prescribe medications at discharge without knowledge of potential unsafe medication interactions.

Another key risk is that data segmentation in response to patient requests will cause clinicians to lose trust in EHRs as sources of truth. As trust erodes, almost every decision will be second-guessed by providers wondering, "What if the EHR is missing important information?" This will unravel the progress we have made as a nation to adopt healthcare IT. Further, it will significantly add to clinicians' workloads because they will need to start from scratch asking for current medications before making treatment decisions. It will also reduce accuracy, should patients not accurately or completely provide their medication lists.

Challenges with Segmentation

Epic takes a "one patient, one record" approach to patient records. Within a health system, each patient has a single record spanning clinical specialties and including a single medication list, a single problem list, and a single set of laboratory results. We have achieved this by building a deeply integrated system atop a single, unified database. Integrated patient records facilitate high-quality cross-disciplinary care and ensure clinicians see the right information at the right time. For example, when a patient presents in a hospital's ED after hours, an integrated chart ensures that ED clinicians have access to the patient's primary care and other outpatient records.

Data segmentation endangers patients and increases clinician workload

With data segmentation, patients no longer have a single, consistent record of care. Instead, information considered "sensitive" by patients is hidden in separate silos that most clinicians cannot access when providing treatment. Any new information entered into such a segmented EHR system must be categorized and placed into the correct silo, a process that cannot be automated because it requires contextual knowledge of *why* the information exists, knowledge that cannot be inferred solely from the data itself.

For example, a female patient asks for restrictions on uses and disclosures of data related to "reproductive health." She has a medication order for misoprostol, commonly used to induce labor. While one might be tempted to automatically silo her misoprostol order as related to her "reproductive health," she may take it for a different indication, such as the prevention of NSAID-induced gastric ulcers.[18] Because many prescribed medications and therapies are approved by the FDA for use for multiple purposes, accurate segmentation will require significant clinical time to carefully review each

[18] https://www.ncbi.nlm.nih.gov/books/NBK539873/

prescription order with contextual knowledge. When this is scaled across the entire health system, the burden is massive. As an example, on a weekly basis in the Epic community, there are over 200,000 allergies documented, 1,260,000 problems identified, and more than 85 million orders written.

No algorithm currently exists to automate the reliable classification of every permutation of data for which patients might request restrictions that result in segmentation. Instead, in response to each individual request, clinicians will need to provide the context to correctly segment and restrict the data. Given the variety (meds, problems, allergies, flowsheets, labs, etc.) and sheer magnitude (more than 100,000 data elements) of health data captured in every patient's chart, this will place a significant burden on clinical staff.

Restricting access to sensitive data weakens evidence-based decision support

By restricting segmented data from other uses, the proposed rule could weaken the application of evidence-based and predictive decision support features that make recommendations based on data in the EHR to prevent certain risks to patients. Medication interaction checking is a key example of such a feature. In the Epic community last year, a medication decision support feature alerted clinicians regarding a contraindication and led clinicians to change their care plans 75 million times.

For example, if a patient requested restriction on uses and disclosures of information around their heart condition, including their medications, and they seek care at an urgent care facility where they are prescribed Levaquin for community-acquired pneumonia, the provider may not receive an alert regarding a potential drug interaction that could cause drug-induced QT prolongation, putting the patient at increased risk of preventable, fatal ventricular arrythmias. Clinicians, knowing that an EHR feature could not be working due to patient-initiated data segmentation blocking their access to critical medication data, will be less likely to trust the system.

Data segmentation strategies will differ across providers

The proposed rule establishes no national standards and provides no guidance on how many data segmentation silos health care providers should utilize nor what information should go into which silo when honoring patient requests for restrictions. High-level categories have been discussed in other venues, but there is no agreed-upon consensus, nor is there agreement regarding how to categorize information that might rightfully fall into multiple categories; to date, suggested categories might include, for example, behavioral health, reproductive health, substance use disorder, and genomics. Each healthcare provider, health IT developer, and patient could create their own categories and definition of what data goes into each category. In practice, segmenting data appropriately will be much more complex than just establishing high-level categories.

Without common definitions among providers, health IT developers, and patients, the likelihood increases for both data leakage (i.e., EHR users accessing data patients do not intend for them to access) and incomplete EHR documentation (i.e., clinicians not seeing data patients thought they

would see). This risk increases even more when data is exchanged between interoperable health systems with differing categories and data components of those categories. As leakage and incomplete EHR documentation are propagated across interoperable health systems, the likelihood grows of reduced provider trust in EHRs and increased risk of harm to patients.

Healthcare providers and IT developers will be on their own to develop access rules

After data has been siloed, each healthcare organization and health IT developer will need a set of rules to fulfill patient restriction requests and determine when and which providers can access segmented data. Consider a patient with a prescription for lithium to treat a mood disorder, which they asked to be segmented as "mental health" information available only to psychiatrists. A cardiologist treating the patient for heart failure may write a prescription for a diuretic that interacts with lithium and could harm the patient.

How should healthcare providers and health IT developers determine rules of conduct when clinicians deem segmenting and restricting data to create risks of foreseeable and serious harms to patients, providers, or members of the general public? Should they honor patients' requests despite the known risks of otherwise preventable and serious harms? Should they "break" the silos and warn certain specialty providers in certain situations? Will they need to create a set of rules covering every potential scenario where a clinician's lack of access to certain information could harm patients or others? It isn't clear how to construct such rules because there are infinite permutations in which healthcare data can interact. It's also unclear how to educate patients on the impacts their individual requests may have on their safety and the safety of others.

Attempts to develop such rules risk creating absurd situations where providers are blocked from seeing information that they created. Consider an OB/GYN clinician who prescribes an antidepressant off-label to treat a patient's premenstrual symptoms.[19] If the patient has requested that "mental health" information be segmented, and antidepressants are automatically siloed as mental health information, the prescription may become unavailable to the clinician—and appear to vanish after it is entered if the clinician cannot access what has been categorized as "mental health information" in the absence of their contextual input. The situation may be further exacerbated if the patient already takes another antidepressant from the same medication class, as prescribed by their psychiatrist, when the OB/GYN clinician places the order to address premenstrual symptoms—unbeknownst to that clinician. Would a dispensing pharmacist have access to information about both prescriptions and be expected to intervene to prevent the potential risk of medication interactions? With which prescribing clinician should the pharmacist communicate about the potential for harm?

[19] https://www.rxlist.com/antidepressants/drug-class.htm

Parsing sensitive data from free-text notes is not feasible

ONC's proposal requires health IT developers to create the ability to segment all USCDI data, which includes unstructured or free-text data such as physician notes, procedure results, and medication instructions. These items may discuss many different aspects of a patient's health, including topics the patient has asked to be segmented.

Data within free-text notes cannot be easily parsed so that specific information in a note is blocked from all but a set of authorized providers. While it is conceivable that Natural Language Processing could partially aid in this problem in the future, we are unaware of any algorithms sophisticated enough to fully and comprehensively address this need under the time frame contemplated by the ONC.

Segmenting sensitive data cannot prevent providers from inferring information from other details in the patient's record

Even if it were possible to accurately and consistently segment data that individual patients consider sensitive, there are many scenarios where clinicians accessing regular, non-segmented data will be able to infer sensitive data from context. For example, a patient might want to segment mental health information related to a schizophrenia diagnosis and clozapine treatment. Because the FDA requires patients taking clozapine to get routine absolute neutrophil count (ANC) lab work, providers could infer a patient is taking this antipsychotic medication when reviewing all recent lab results.

Every time a patient asks for data to be segmented, the clinician or healthcare organization would need to consider every inference that could be made from indirect data. Consider just a few examples of subjective judgment calls that would be needed:

- A patient requests restrictions for information related to their sexuality. If that patient received a vaccine based on meeting one of the CDC recommended criteria of recent sexual activity, should that vaccination information be segmented because a physician could *infer* sexuality?
- A patient requests restrictions for their reproductive health information. If that patient develops a deep vein thrombosis (DVT) due to an oral contraceptive, should the history of DVT be hidden from their problem list?
- A patient requests restrictions for their data related to a condition they deem sensitive. If that patient takes a medication related to that condition, such as lorazepam for anxiety, and has an allergic reaction or experienced a severe side effect that warrants discontinuing the medication, should the medication be displayed in the patient's allergy/contraindication section?
- A patient requests restrictions for their reproductive health information, including a pregnancy. If that patient develops gestational diabetes, should the episode of gestational diabetes be displayed to endocrinologists who are not authorized to see reproductive health information?

It is also unclear how ONC would reconcile inclusion of segmented information in decision support with transparency requirements that are included in the Decision Support Intervention section of this proposed rule. A user who is restricted from siloed data may be able to infer the data from source attribute or risk management information. Should segmented information pertinent to an algorithm not be included as an input to the predictive model, making it less effective? Should the information be included but clinicians be precluded from seeing the output from the decision support? Should clinicians not be allowed to see the inputs to the advisory to understand the basis for the output of the decision support?

Patient Issues

If a healthcare provider segments and restricts data as requested by a patient, the patient will expect all of their healthcare providers to keep that commitment, every time. Patients who have been promised that only psychiatry clinicians will see their mental health data will interpret that promise as violated when data is misclassified, leaked through a free-text note, determined from inferential data, or presented as part of clinical decision support to clinicians in other specialties. Patients will lose trust in the healthcare system as a whole when providers they interact with do not follow consistent processes when addressing restriction requests.

Research shows that a high level of distrust already exists in the U.S. healthcare system and determined a close association exists between distrust and poor health.[20] We are concerned that data segmentation, as contemplated in the proposed rule update, will further undermine trust in the U.S. healthcare system, leading patients to withhold information from clinicians and avoid seeking care for preventable and treatable conditions.

Patients will encounter piecemeal systems that cannot guarantee certain data will never be shared.

There is no requirement in the ONC proposal that providers be required to agree to patients' requests to restrict uses or disclosures of their protected health information, or that healthcare providers or health systems protect sensitive data in the same ways. Further, this proposal relates only to certified health IT, and there are many other places inside and outside of traditional healthcare settings where health data is stored and accessed. For example, patient data is routinely used for medical billing, fulfilling orders for medications and durable medical equipment, research, and other purposes. Payers, retail pharmacies, DME vendors, and other groups working with patient data often rely on their own information systems, which are not certified health IT.

Public health entities also frequently use and disclose patient data. Should information about vaccinations that patients seek to restrict from certain uses be withheld from immunization registries? Should state health portals, which are not certified health IT, be required to segment data in response to restriction requests? If not, what happens in states where healthcare providers and public health agencies exchange immunization information through bi-directional interfaces? Providers could receive information from state registries that patients did not want them to see.

[20] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1484714/

Rather than providing guidance or flexibility, ONC is tossing a hot potato to overburdened health systems and providers and asking them to navigate this complex landscape and deal with any potential fallout. We are concerned that ONC is avoiding its statutory responsibilities to develop policy consensus and is instead shifting those responsibilities to health systems and healthcare providers.

Proposed Alternative

ONC proposes to take an incremental step forward by requiring health IT developers to develop "discrete parts" of privacy "workflows."[21] From our health IT developer's perspective, ONC's proposal is unworkable.

- There is no "incremental" approach to data segmentation that would enable a user to flag all USCDI (including unstructured free-text data like physician notes) and prevent any flagged data from being used or disclosed for a restricted purpose. To even attempt what ONC is proposing, health IT developers would have to rewrite underlying EHR systems; this may require significant reconfiguration of EHR systems by health systems that have already invested significant sums in implementing EHRs to meet their needs. This would result in extraordinary costs to already overburdened health systems—and may delay health IT developers from pursuing more innovative healthcare solutions to leverage new and emerging technologies that show promise for improving the efficient delivery of high-quality healthcare.
- The proposed rule update ignores critical technology and policy challenges with unstructured and inferential data that are key to "enabl[ing] a user to implement a process to restrict uses or disclosures of data in response to a patient request."[22]
- We are certain that the level of assurance ONC wants to provide patients who request restrictions on uses or disclosures of their protected health information is not realistically achievable—with either structured or unstructured data.

ONC should advance clinically, financially, and technically feasible privacy solutions

To have the best opportunity for success, ONC should take a more measured and evidence-based approach by focusing on a set of key patient privacy use cases that health IT developers and healthcare providers are already working to address today.

Introduce granular certification controls on proxy access to patient portals

Pediatric healthcare providers using Epic EHRs have encouraged us to develop proxy access controls for purposes such as protecting the privacy of adolescent patients suffering from abuse, for example, taking steps to ensure patients and providers control who obtains proxy access to patient records and

[21] Notice of Proposed Rulemaking, Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing, P. 23821 of Federal Register Vol. 88, No. 74, Tuesday, April 18, 2023.
[22] Id at 23822.

the degree of information available to such proxies. We encourage ONC to participate in this policy discussion, foster development of consensus across healthcare providers, and propose certification requirements that afford pediatric patients throughout the country access to the same privacy protections. As specific access controls are proposed in future regulation, developers will be able to estimate a reasonable time frame for implementation of any necessary updates.

Add certification requirements for segmentation of certain sensitive notes

While parsing sensitive data inside of free-text notes is not feasible, ONC could introduce certification requirements focused on granting healthcare providers the option to segment entire discrete sensitive notes. This would allow clinicians to limit access to notes that patients consider sensitive, in a fully self-contained way. For any patient records that contain sensitive notes, there should be an alert that indicates such records contain restricted information. In this scenario, we also recommend that ONC require a designated point of contact for that restricted information (such as the clinician who limited access to the information or an ombudsperson). In this scenario, a clinician who does not have access to the sensitive note could ask someone who does have access to this information to assess medication orders for contraindication, if desired. Sensitive notes restricted from sharing through interoperability tools and restricted from proxies with patient portal access would also offer clinicians opportunities to explore and better understand the potential benefits and risks of limiting access to certain notes, as well as help ONC to generate data to better inform future policies on patient-requested restrictions and resulting data segmentation of certain protected health information. This requirement would be practical to add to certification on the proposed 1/1/2026 time frame.

Conclusion

ONC should rework its entire proposal, taking into consideration established clinical standards, technical capabilities, policies, and settled understandings regarding the safe and efficient delivery of high-quality healthcare. ONC's proposals are not workable and will place patients and healthcare providers at risk of serious harms. Patient medical records should be sources of truth. As an alternative, ONC should introduce granular certification requirements for proxy access to patient portals and add requirements for discrete sensitive notes.

Should ONC proceed with its current proposal for certification criteria in support of patient requested restrictions on uses and disclosures of protected health information despite the potential risks outlined herein, we recommend the date for new certification criteria regarding patient-requested restrictions be moved from January 1, 2026, to January 1, 2030, given the significant work required by health IT developers and reconfiguration of EHR systems that will be required of health systems. We conservatively estimate it will take up to 1,000,000 hours of development time plus significant ongoing annual maintenance to comply with ONC's requirements as proposed. The hours needed for implementation work for health systems and healthcare providers will be in addition to those estimates.

OptumInsight

11000 Optum Circle
Eden Prairie, MN 55344

Optum.com

October 4, 2023

Ben Steffen
Commissioner
Maryland Health Care Commission
4160 Patterson Ave
Baltimore, MD 21215

Commissioner Steffen,

OptumInsight is pleased to submit comments in response to the Code of Maryland Regulations (COMAR) 10.25.07 as proposed by the Maryland Health Care Commission (MHCC). The proposed rules address privacy protections for the exchange of health care information. OptumInsight is the largest clearinghouse operating in Maryland and a certified Electronic Health Network (EHN) under both our Legacy Change Healthcare brand and our OptumInsight brand. We appreciate the opportunity to provide informal comments on this important proposed regulation.

OptumInsight provides data, analytics, research, consulting, technology and managed services solutions to hospitals, physicians, health plans, governments and life sciences companies. This business helps customers reduce administrative costs, meet compliance mandates, improve clinical performance and transform operations.

We strongly support protecting patients' sensitive health information. We have participated in the SHIFT task force since its inception to support the development of industry standards for appropriately restricting sensitive health information and make every effort to secure and protect patient data throughout its lifecycle. The task force includes representatives from provider organizations, health IT vendors, government agencies, legal and policy groups, and patient advocates working to drive standards development, implementation guidance, and policy to advance patient-driven sharing of information. We generally agree with MHCC's proposed changes to COMAR 10.25.07 and offer the following comments that we believe will add clarity to and create a shared understanding of the requirements. We are also happy to meet with MHCC to discuss our comments and answer any follow-up questions.

COMAR 10.25.07.02 Definition of Adjudication of Claims

COMAR 10.25.07.05 conditions certification, in part, on the provision of "(c) [] an attestation signed by an officer of the applicant that the applicant restricts disclosure of legally protected health information as required by Health-General Article, §4-302.5, Annotated and COMAR XX.XX.XX". Section 4–302.5 includes an exemption to its general prohibition on certain disclosures for (1) for the adjudication of claims. We strongly support this exemption since it enables appropriate transactions to flow between covered entities to ensure payment for covered services. However, we are concerned that neither the law nor the proposed modifications to COMAR 10.25.07 define adjudication of claims. We believe that all X12 transactions an EHN sends between Covered Entities and other EHNs are related to the adjudication of claims, since they are all components leading to an approved or denied claim and the subsequent payment. For example, an eligibility transaction is the first step that communicates a patient's coverage status to a healthcare provider, before care is given, so that there can be a successful claim after the encounter. Consequently, we would consider the eligibility transaction to be related to the adjudication of claims.

We are concerned that without an appropriate definition, EHNs could be prohibited from sharing necessary transactions with payers to enable them to pay for the care they are mandated to provide in Chapter 249. A single encounter typically has a minimum of 10 transactions between providers and payers, starting with the patient scheduling the visit or showing up for care, the actual encounter and documentation of the encounter, and any follow-up care such as lab tests, prescriptions, imaging studies, etc. X12 specifies different transactions that cover this entire process from eligibility to prior authorization to claim submission and documentation submission to remittance advice and payment. If even one of the transactions in the series are not considered adjudication of claims by MHCC, the claim ultimately may not be processed, requiring patients to pay out of pocket for services payers are required to

cover. We recommend that MHCC explicitly recognize the exemption provided for the adjudication of claims in §4-302.5, and include a definition for adjudication of claims that is to enables all of the necessary transactions to flow. For example, the definition could enumerate the claims processing functions EHNs perform identify (as noted in the MCC's Electronic Health Networks Overview Flyer (2023) similar to the HIPAA Privacy Rule defines for Payment.[1]

COMAR 10.25.07.02B(8)

"Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including (a) Mifepristone data, as defined by the Secretary, and (b) As provided in COMAR XX.XX.XXX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.

> We agree with this definition; however, we are concerned about the timing of the first attestations in December of this year, without clear guidance regarding the defined data that would be considered Sensitive Health Services. We anticipate that the list of data will be extensive and complex, and we are concerned that we may be required to attest we have technology in place without knowing what data must be restricted. We encourage MHCC to move quickly to determine the initial list of data and develop a standard process for updating the list in accordance with standards development organizations (SDOs) such as X12.

COMAR 10.25.07.05A(2)(c)

Provide an attestation signed by an officer of the applicant that the applicant restricts disclosure of legally protected health information as required by Health-General Article, §4-302.5, Annotated and COMAR XX.XX.XX.

> As discussed above, we believe that all the transactions an EHN discloses are related to the adjudication of claims. Consequently, we recommend that MHCC amend the attestation to the following: *Provide an attestation signed by an officer of the applicant that the applicant restricts disclosure of legally protected health information as required by Health-General Article, §4-302.5, Annotated and COMAR XX.XX.XX or that the applicant is exempted from such restrictions under Health-General Article, §4-302.5(B)(1).*

COMAR 10.25.07.09B

An MHCC-Certified EHN must report on compliance progress to the Commission. (1) By December 18, 2023, an MHCC-certified EHN shall submit to the Commission: (a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX;

> We recommend that MHCC add a new (b) section to the above. The full text we recommend is:
>
> *An MHCC-Certified EHN must report on compliance progress to the Commission.*
>
> *(1) By December 18, 2023, an MHCC-certified EHN shall submit to the Commission:*
>
> *(a) An affirmation that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX; or*
>
> *(b) An affirmation that it is exempted from filtering and restricting disclosure of legally protected health information under Health-General Article, §4-302.5(B)(1); or*
>
> *(c) An implementation plan that includes….*

The proposed rule further provides that the implementation plan must include: (i) An affirmation that despite its best efforts, the MHCC-certified EHN lacks the technological capability to fully comply with Health-General Article, §4-302.5, Annotated Code of Maryland as of December 1, 2023, including a detailed explanation of the EHN's limitations.

> We generally support the submission of an implementation plan for EHNs who do not meet the exemption under Health-General Article, §4-302.5(B)(1) and who do not have technology in place by December 18, 2023. However, we are concerned with the language above requiring an "affirmation of best effort." This

language is nebulous and subjective, and it is unclear what MHCC would consider an organization's best effort.

As discussed above, OptumInsight (legacy Change Healthcare) has been a participant in the SHIFT task force since its inception. One of the goals of the task force is to build standards for data segmentation of sensitive health information, particularly to enable appropriate data sharing with parents, guardians, and caregivers. The task force has been meeting for more than two years, and it still has not been able to gain consensus on standard methods for segmenting discreet data elements that would be considered sensitive health information. It is incredibly difficult from both an informatics perspective (which data should be segmented) and a technical perspective (how to tag data appropriately and determine who should have it). Additionally, the X12 standards do not currently provide any means for segmenting data, and even FHIR is in early stages with segmentation with no real-world implementations. Further, as EHNs, many of our services are a "pass through" of data from one end-point to another. In most cases, we do not open up the transactions (though a small number of our more advanced products do, such as our claims editing tools). This adds further technical complexity to having a solution in place.

Based on the above, we recommend that MHCC more clearly define or remove the *best efforts* language from the provision.

We appreciate MHCC's consideration of the above comments. We recognize the complexity of these new requirements, and we are looking forward to working with MHCC to create a shared understanding of how we can best protect patients' sensitive health information. Please contact <insert name> for follow-up questions or to schedule a meeting.

Sincerely,

Robert D. Morrow Jr.

ORACLE
Health
8779 Hilcrest Road,
Kansas City, MO 64138
Direct: (816) 201-1024
Fax: (816) 474-1742

Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

October 4, 2023

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

10.25.07.02.B.8 & 10.25.18.02.B.40

"Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including (a) Mifepristone data, as defined by the Secretary, and (b) As provided in COMAR XX.XX.XXX, the diagnosis, procedure, medication, and other codes related to: (i) Abortion care; and (ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland

Without specifying code values related to clinical concepts (ex: the following ICD-10 codes for diagnoses, SNOMED CT code values for problems, LOINC codes for Lab Results, etc.), the burden of identifying codes related to abortion care and sensitive health services is placed on the clinician who is performing the action and/or adding the respective data to the record. This creates supplementary tasks and an unnecessary burden on the clinician to define what constitutes abortion care or sensitive health services. Without clear definitions, clinicians are unlikely to reach the same consensus of what constitutes "related to abortion care" or "sensitive health services," generating an inconsistent standard across Maryland-based health care organizations.

Health IT vendors (who may qualify as EHNs or HIEs) are also unable to provide technology solutions to reduce the burden of identification of abortion-related or sensitive health codes for the clinicians if the codes haven't been explicitly defined. While diagnoses, procedure, and medications are specifically identified as clinical concepts subject to these restrictions, "other codes" is not specific enough for Health IT vendors to be able to create technical solutions to provide to Maryland-based health care organizations.

Clinical data is stored on database tables. For data to be processed and authorized/not authorized for action to be taken on the data (access, transmission, modification, deletion, etc.), certain metadata or attributes must be associated to the clinical data. Without having the entire list of specific clinical data sets – like diagnoses, procedures, medications – defined, database infrastructure cannot be updated or modified to support the necessary metadata/attributes that will allow a health IT system to make an authorization decision to determine if this information is relevant to the law and subject to the authorization decision.

Oracle provides the following Recommendations.

1. Removal of the phrase "other codes" and replace with all specific clinical data types – like diagnoses, procedures, and medications – that should be applicable to the law.
    a) Identifying all the applicable clinical data types will enable IT vendors to update their infrastructure in support of authorization functionality to meet the law's intent to control access and transmission to data.
2. Within the applicable clinical data types, all the intended abortion-related and sensitive codes should be identified.
    a) Identifying the specific values will eliminate ambiguity for clinicians and clarify if a specific, discrete piece of data is abortion-related and/or sensitive. Identifying the specific values will also enable IT vendors to develop functionality that can automatically flag those specific values as subject to this law, reducing (possibly altogether removing) the chance of data becoming inappropriately accessible due to clinician or process error.
    b) If specific clinical data types and specific clinical data codes are not explicitly defined, health organizations will likely be forced to conservatively restrict the entire patient

record from being accessible and/or transmissible whenever there is a chance that a record contains anything that could be identified as abortion-related or sensitive. Restricting access/transmission to a patient's entire record due to the chance that some data within the record could be defined as abortion-related or sensitive will result in many records losing interoperability currently in place. This could impact a providers informed medical decision-making ability and the patient quality of care.

10.25.07.09.B & 10.25.18.04.C

"Beginning December 1, 2023, an HIE or EHN is prohibited from disclosing mifepristone data or the diagnosis, procedure, medication, or related codes for abortion care and other sensitive health services (as determined by the Secretary) to a treating provider, a business entity, another HIE, or another EHN, unless the disclosure is (1) for the adjudication of claims or (2) to a specific treating provider at the written request of and with the consent of a patient, parent, or guardian, as specified."

Patient, parent, or guardian consent lacks specificity needed to provide a consistent approach across the impacted health organizations of Maryland.

For information that is authorized or restricted from transmission outbound from a health organization, having a set of specified best practice standards ensures:

1. Patient-understanding of how their data is handled and/or processed, what the consent means, and what it enables a healthcare organization to do with their data.
2. Healthcare Organizations have a common understanding of what pieces of patient information should be captured as part of the consent, at what point in the patient's journey the consent should be captured, and what consent information should be passed from the capturing organization to a recipient organization, for instances where the consent for patient data transmission exists.

If consent specifics are defined, IT vendors can better provide solutions that:

1. Ease the capture of consent for healthcare personnel by providing locations to capture the consents that are native to the workflow.
2. Store the consents in the database in a manner that can automate the consent policy check prior to allowing abortion-related or sensitive data transmission.

With outbound data transmissions occurring via HL7, FHIR, or other interface transactions already automated, if the consent policy check isn't automated as well, then the current automated transmissions (for all data, not just abortion-related and sensitive data) will likely need to cease, so a manual consent check can take place. A manual consent check will require more staffing to perform these checks prior to approving outbound data transmission and could create risk for the patient's privacy through human error.

Oracle provides the following recommendations.

1. Provide consent policy specifics:
    a. What fields must be captured with the consents.
        i. Additionally for IT vendors, identify if there are technical specifications to storing the consent.

b. How often consents expire or need to be renewed.
c. Guidance on when the consents should be captured.
d. If the consents should be included with the transmission of the data from a sending organization to a receiving organization.
e. If a consent is needed from a receiving organization for purposes of re-disclosure to another organization.
f. Ideally, the consent could be captured from any EHN or HIE in the state, but the consent would be stored at the state-level – creating a singular, interoperable source of truth for the patient's consent.
    i. For the patient, this means they must only provide consent once for any abortion-related or sensitive data transmission – instead of separate consents for each MD-based health organization where the patient that may have abortion-related or sensitive data captured at or received via transmission.
    ii. For healthcare organizations, it means there is one source of truth for the patient and lowers possible inappropriate disclosure of abortion-related or sensitive data because they don't have to maintain their own consent for that patient's data – rather the healthcare organizations would rely on what the patient's wishes are, as stored at the state-level.
    iii. For IT vendors, it enables them to query a common source of truth and have confidence that consent being used by one healthcare organization won't be overridden or come into conflict with a consent captured and being used by another organization.

10.25.07.09.C & 10.25.18.09.C.3

Beginning June 1, 2024, a person who knowingly violates Health-General Article, §4-302.5, Annotated Code of Maryland, shall be guilty of a misdemeanor and on conviction is subject to a fine not to exceed $10,000 per day.

The time from bill passage June 1, 2023, and the law's requirements going into effect on December 1, 2023 (6 months), as well as the introduction of a financial penalty up to $10,000 per day on June 1, 2024 (12 months), leaves healthcare organizations little time to put new processes into place and/or develop new technology to meet the new requirements.

IT vendors in the healthcare industry must inherently be more cautious when developing new functionality than other industries due to the nature of healthcare tech and the severity of problems that can occur when the development is rushed and/or pushed out prior to adequate validation and performance testing. As such, it is common practice at a national-level to allow for 18-24 months for IT vendors to develop new features and capabilities to support data-level access controls.

New technology development timeline concerns include the following:

1. To support the law's requirements, IT systems will need the ability to:
    a) Identify abortion-related and sensitive data from their applications and program user interfaces.
    b) Write and store metadata identifying a particular piece of data as abortion-related or sensitive.
    c) Recall the stored metadata when performing an evaluation of whether a transmission is authorized or not.

d) Perform a consent check to understand that if data that is identified as abortion-related or sensitive is permitted to be transmitted.
    i. If the consent capability isn't handled by an IT system, it will require manual checking for every outbound transmission.
e) Ensure that for any data that is identified as abortion-related or sensitive to which the patient has NOT consented for transmission is restricted from transmission across all the outbound data channels a healthcare organization has in place including, but not limited to HL7, FHIR, custom interfaces, and more.
    ii. Some IT vendors may support some of these capabilities today, but to support all of them for all the possible data types that could include abortion-related or sensitive data and account for all the possible outbound transmission channels, it will require some development from a large majority of IT vendors.

If adequate time to develop the features to support the law is not considered, it will result in:

a) Rushed development of new features likely being deployed to the market without adequate performance or functional testing.
b) Limited features being released to the healthcare organizations with manual, human workarounds and processes to fill the gaps that the vendors didn't have time to safely develop.
    i. These manual, human workarounds will cost organization time and money to deploy and train and will introduce variance and risk to the data inappropriately being transmitted.
c) Due the complex technical infrastructure in place for healthcare organizations, the change control process when implementing anything new (e.g., process, application, device, etc.) is critical.
d) Not having adequate minimum system or personnel requirements in place means the new process or technology could fail. If things fail for a healthcare organization it can mean loss in critical revenue, data breaches, staff endangerment, and even patient safety events (including death). For this reason, healthcare organizations mitigate these risks by:
    i. Limiting the frequency of large process or technology changes, and
    ii. Having a long preparation period prior to the change to make sure all the necessary steps are in place to make the change.
e) It's common practice for healthcare organizations to only implement whole-scale process change or install new technology once or twice a year – giving themselves 6-12 months to prepare for a cutover period at which the change is implemented. Preparations steps may include, but aren't limited to:
    i. Staff training for the new process or technology (larger the organization, the more challenging it is to train all staff).
    ii. Device upgrades to ensure the adequate hardware is in place for the new process or technology.
    iii. Software upgrades to ensure that a new program is compatible with existing applications.
    iv. Facility upgrades to ensure that buildings and other physical infrastructure is in place for the change.
    v. Command center coverage to make sure that there is a first response team in place for the actual cutover change time-period.

vi. Front-line support to mitigate and address issues that occur during the change.
vii. Ensuring there aren't overlapping conflicts/plans with other changes or major events that could result in the change not successfully taking hold.

f) Due to the necessary preparation for change needed, most organizations have identified what changes are planned to their system anywhere from 12-36 months in advance, with larger changes planned even beyond that timeframe.
    i. As stated, the introduction and requirement of material changes to the processes and technology of a healthcare organization within 6 months (effectively) and 12 months (with financial penalties), could lead to inadequate preparation before deploying these changes.

Without adequate time to develop the technology and processes needed to comply with the law, healthcare organizations could experience adverse outcomes and may inappropriately transmit a patient's abortion-related or sensitive data outbound from the healthcare organization.

Patient First

October 4, 2023

Send via email anna.gribble1@maryland.gov

Anna Gribble
Maryland Health Care Commission
Program Manager
4160 Patterson Avenue
Baltimore, Maryland 21215

Re: Comments of Patient First Corporation regarding Draft COMAR 10.25.18.01 *et seq.* "Health Information Exchanges: Privacy and Security of Protected Health Information"

Dear Ms. Gribble:

Thank you for the opportunity to submit comments on the September, 2023 draft of COMAR 10.25.18.01 *et seq.* "Health Information Exchanges: Privacy and Security of Protected Health Information," which is separately entitled Unofficial Draft Emergency Regulations in Support of HB 812: Health – Reproductive Health Services – Protected Information and Insurance Requirements (the "Draft Regulation").

At the outset, we note that the Draft Regulation is substantially similar, but not identical to, draft regulations previously published on May 24, 2023 (the "May Regulation"), to which Patient First previously submitted comments by letter dated June 19, 2023 (copy enclosed). We understood, based on your office's comments in July, that you hoped to convene stakeholder discussions regarding the May Regulation this fall. We are disappointed that the MHCC has incorporated the same provisions in the Draft Regulation that Patient First addressed in its comment letter to the May Regulation without responding our concerns or having any discussions with us.

Patient First is therefore resubmitting its prior comments with respect to both the May Regulation and the current Draft Regulation:

Patient First Corporation and its affiliated medical groups (collectively, "Patient First") operate 24 medical care centers in Maryland, at which we provide primary and urgent care services to over one million Maryland patients annually (including over 250,000 Medicaid visits). Our medical centers are open 7 days a week from 8 a.m. to 8 p.m. every day of the year. In addition to our primary and urgent care services, we offer moderate complexity laboratory testing, on-site diagnostic services, including EKG and x-ray, prescription drugs and durable medical equipment and supplies.

For the purposes of the Draft Regulation (and the May Regulation), Patient First uses a proprietary electronic medical record, the Physician Assistance System ("PAS"), that it developed and improved over the past 40 years. The PAS is an ONC Certified Health Information Technology that was most recently re-certified on December 22, 2022.[1] Use of the PAS is limited to Patient First medical centers; Patient First does not market, sell or license use of the PAS in the state of Maryland outside of its 24 Patient First medical centers, which operate as an organized health care arrangement as that term is defined in 45 CFR §160.103.

Our review of the Draft Regulation and statutory provisions of the Maryland Code indicate that Patient First would not be regulated as an HIE because it is an organized health care arrangement. Specifically, under the Draft Regulation an HIE includes "a health information technology developer of certified health information technology" [at .01.B(1)(b)]. However, under Section 4-301(i)(2) of the Health - General Article, the term 'health information exchange' does not include "an entity composed of health care providers under common ownership if the organizational and technical processes the entity provides or governs are for health care treatment, payment or operations purposes, as those terms are defined in 45 CFR §164.501". Section 4-301(i)(2) then defines 'common ownership,' in part, as ownership of a health care entity "by health care organizations operating as an organized health care arrangement, as defined in 45 CFR §160.103". Therefore, because Patient First uses the PAS to perform functions described in the definition of 'health care treatment, payment or operations" and comprises health care organizations operating as an organized health care arrangement, each as defined in the Maryland Code, Patient First is excluded from those provisions of the Draft Regulation that are applicable to a HIE.

However, because a violation would be punishable by penalties of up to $10,000 per day per affected individual and the detrimental harm that it would have on patient care if Patient First was required to comply with these draft regulations, Patient First is requesting clarifying language. To illustrate one situation where detrimental harm would occur if Patient First was categorized as an HIE under these draft regulations for compliance purposes, Patient First would be required to offer patients the ability to opt out of participation in the PAS or to limit the health information contained in the PAS. As noted above, the PAS literally is the medical record for health care services provided at Patient First to over a million Maryland patients annually. We have no ability to provide care without the use of the PAS to create a medical record (and doing so would be contrary to principles of medical ethics and the standard of care). With over a million patients a year, it is clear that any dispute regarding applicability of the HIE provisions of the Draft Regulation to Patient First is a life-or-death proposition for our employees and patients.

Therefore, we propose the following clarifications to the Draft Regulation:

- Add the following text as a new Section .01.D:

[1] ONC-ACB Certification ID 15.04.04.2140.PAS1.15.02.0.221212; please see the ONC's Certified Health Product List at https://chpl.healthit.gov/#/listing/11065 for additional information regarding the PAS.

Sections .02 through .12, inclusive, of this chapter do not apply to a health information technology developer, as described in .01.B(1)(b), that sells, licenses or otherwise provides certified health information technology within the State of Maryland exclusively to and as a part of a group of entities under common ownership as defined at Health-General Article 4-301, Annotated Code of Maryland.

- Add the following as a new .01.C(3):

A health care entity (including a health care entity that meets the definition of HIE hereunder) that is engaged in the provision of management services to an affiliated health care provider or providers, including selling, licensing or otherwise providing certified health information technology, if the health care entity and its affiliated providers operate under the same trade name.

Patient First recognizes the difficult task in discerning the various electronic systems used in today's complicated health care delivery system. We believe that the addition of the above language conforms to the exclusions in Maryland's law and the draft regulation and provides greater clarification. We appreciate your support. If you have any questions, please don't hesitate to contact me at 804-822-4490. Thank you.

Sincerely,

Stephen C. McCoy
Vice President/General Counsel

Enclosure

cc: Danna Kauffman, Schwartz, Metz, Wise & Kauffman, P.A.

Patient First

June 19, 2023

Send via email anna.gribble1@maryland.gov
Anna Gribble
Maryland Health Care Commission
Program Manager
4160 Patterson Avenue
Baltimore, Maryland 21215

Re: Draft Regulation Discussion Document: "Health Information Exchanges: Privacy and Security of Protected Health Information"
Comments from Patient First Corporation

Dear Ms. Gribble:

Thank you for the opportunity to submit comments on the May 24, 2023 draft regulation discussion document entitled "Health Information Exchanges: Privacy and Security of Protected Health Information" (the "Draft Regulation").

Patient First Corporation and its affiliated medical groups (collectively, "Patient First") operate 24 medical care centers in Maryland, at which we provide primary and urgent care services to over one million Maryland patients annually (including over 250,000 Medicaid visits). Our medical centers are open 7 days a week from 8 a.m. to 8 p.m. every day of the year. In addition to our primary and urgent care services, we offer moderate complexity laboratory testing, on-site diagnostic services, including EKG and x-ray, prescription drugs and durable medical equipment and supplies.

For the purposes of this draft regulation, Patient First uses a proprietary electronic medical record, the Physician Assistance System ("PAS"), that it developed and improved over the past 40 years. The PAS is an ONC Certified Health Information Technology that was most recently re-certified on December 22, 2022.[1] Use of the PAS is limited to Patient First medical centers; Patient First does not market, sell or license use of the PAS in the state of Maryland outside of its 24 Patient First medical centers, which operate as an organized health care arrangement as that term is defined in 45 CFR §160.103.

Our review of the Draft Regulation and statutory provisions of the Maryland Code indicate that Patient First would not be regulated as an HIE because it is an organized health care arrangement. Specifically, under the Draft Regulation an HIE includes "a health information technology developer of certified health information technology" [at .01.B(1)(b)]. However, under

[1] ONC-ACB Certification ID 15.04.04.2140.PAS1.15.02.0.221212; please see the ONC's Certified Health Product List at https://chpl.healthit.gov/#/listing/11065 for additional information regarding the PAS.

Section 4-301(i)(2) of the Health - General Article, the term 'health information exchange' does not include "an entity composed of health care providers under common ownership if the organizational and technical processes the entity provides or governs are for health care treatment, payment or operations purposes, as those terms are defined in 45 CFR §164.501". Section 4-301(i)(2) then defines 'common ownership,' in part, as ownership of a health care entity "by health care organizations operating as an organized health care arrangement, as defined in 45 CFR §160.103". Therefore, because Patient First uses the PAS to perform functions described in the definition of 'health care treatment, payment or operations" and comprises health care organizations operating as an organized health care arrangement, each as defined in the Maryland Code, Patient First is excluded from those provisions of the Draft Regulation that are applicable to a HIE.

However, because a violation would be punishable by penalties of up to $10,000 per day per affected individual and the detrimental harm that it would have on patient care if Patient First was required to comply with these draft regulations, Patient First is requesting clarifying language. To illustrate one situation where detrimental harm would occur if Patient First was categorized as an HIE under these draft regulations for compliance purposes, Patient First would be required to offer patients the ability to opt out of participation in the PAS or to limit the health information contained in the PAS. As noted above, the PAS literally is the medical record for health care services provided at Patient First to over a million Maryland patients annually. We have no ability to provide care without the use of the PAS to create a medical record (and doing so would be contrary to principles of medical ethics and the standard of care). With over a million patients a year, it is clear that any dispute regarding applicability of the HIE provisions of the Draft Regulation to Patient First is a life-or-death proposition for our employees and patients.

Therefore, we propose the following clarifications to the Draft Regulation:

- Add the following text as a new Section .01.D:

  Sections .02 through .12, inclusive, of this chapter do not apply to a health information technology developer, as described in .01.B(1)(b), that sells, licenses or otherwise provides certified health information technology within the State of Maryland exclusively to and as a part of a group of entities under common ownership as defined at Health-General Article 4-301, Annotated Code of Maryland.

- Add the following as a new .01.C(3):

  A health care entity (including a health care entity that meets the definition of HIE hereunder) that is engaged in the provision of management services to an affiliated health care provider or providers, including selling, licensing or otherwise providing certified health information technology, if the health care entity and its affiliated providers operate under the same trade name.

Patient First recognizes the difficult task in discerning the various electronic systems used in today's complicated health care delivery system. We believe that the addition of the above language conforms to the exclusions in Maryland's law and the draft regulation and provides greater clarification. We appreciate your support. If you have any questions, please don't hesitate to contact me at 1-804-822-4490. Thank you.

Sincerely,

Stephen C. McCoy
Vice President/General Counsel

cc: Danna Kauffman, Schwartz, Metz, Wise & Kauffman, P.A.

PUBLIC POLICY PARTNERS
INNOVATIVE POLICY SOLUTIONS

October 4, 2023

Anna Gribble
Program Manager
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215

Dear Anna:

Thank you for your continued work on implementation the provisions of HB 812/SB 786 from the 2023 session. I appreciate the Commission's commitment and expediency in making sure the legislation is implemented. Almost 20 states have abortion bans in place, and more are pending. It is critical that we protect consumers seeking abortion and other legally protected care in Maryland by keeping their personal health information from being shared over state lines.

Thank you for the opportunity to review and provide comments to the draft regulations for COMAR 10.25.07 and 10.25.18:

1) **No Exemptions Allowed Under Statute for Complying with Legally Protected Health Care Requirements:** Under 10.25.18.01(D), the draft regulations delineate that a health information exchange could require an exemption from the legally protected health care requirements. The statute enacted under HB 812/SB 786 does not provide the Maryland Health Care Commission with the authority to allow for exemptions from the legally protected health care requirements. I would request that this provision be removed from the draft regulations or modified to clarify that there are no exemptions from the legally protected health care provisions.

2) **Technical Correction***:* Under 10.25.07.02(B)8(b)(ii) and 10.25.18.02(B)(40)(b)(ii), the reference to statute should be "4-310".

3) **Secure Third-Party Transactions Regarding Consumer Education Materials:** Under 10.25.18..03(B)(4), the draft regulations modify current requirements regarding the availability of consumer education materials: "An HIE shall make health care consumer educational materials readily available, *at no charge,* to participating organization and [their users] *the participating organizations' users through distribution channels such as websites, postal mail, email, secure third-party smart phone applications, and other reasonably media or distribution channel commonly used and generally available to the HIE and health care consumer."* I strongly recommend additional protections on the sale or redisclosure of data related to consumer requests regarding protections for legally protected health care. HIEs should be required to have agreements with any of these third-parties to prohibit the sale or redisclosure of consumer requests regarding legally protected health care. There should be close examination of whether these entities already are or should be prohibited from providing this information in response to an out-of-state investigation of legally protected health care. While Maryland's law would likely prohibit such an action *in Maryland*, some of these third party vendors could be located outside of our state.

4) **Exceptions to the Information Blocking Rule:** Under 10.25.18.04.A(3)b, the draft regulations have rewritten the provision related to disclosure of sensitive health information. The revised language reads, "*If a federal or State law does not require written consent or authorization for the access, use, or disclosure of the sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE."* I wanted to raise a question about how this newly written provision may interplay with the federal exceptions under the Information Blocking Rule. Would the newly written provision interfere in any way a provider deciding to block information under one of the exceptions, such as the preventing harm or privacy exceptions?

5) **More Specificity about Compliance:** Under 10.25.18.04.(C), the draft regulations delineate a series of affirmation and reporting requirements throughout the implementation process. I would suggest that a HIE should affirm that it is compliance with the law by protecting legally protected health care through the segregation of data by code, rather than blocking of the electronic health record of the consumer who has received legally protected care or who meets certain demographic criteria (e.g. age and gender). This change should be made to align this section with the statutory requirements.

Similarly under 10.25.07.05 and 10.25.07.09(B), the attestation and reporting requirements for compliance for EHNs should also have more specificity to align it with the statutory requirements.

6) **Clearer Audit Requirements Regarding Legally Protected Care:** Under 10.25.18.06, the draft regulations delineate a series of audit requirements. I would recommend providing specificity around the HIE's compliance with protecting abortion care and other legally protected health care by segregating data by procedure, medication, or related codes.

7) **Requirements for Accessing, Using, or Disclosing Data Through and HIE in an Emergency;** Under 10.25.18.06, I would recommend for clarity's sake to add a provision specifying that this section does not apply to legally protected care.

Thank you for the opportunity to submit these comments. If any other information is helpful, please just let me know. I may be reached at relliott@policypartners.net.

Sincerely,

Robyn Elliott
Managing Partner

October 4, 2023

Submitted electronically via:
Mhcc_regs.comment@mhcc.gov

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

RE: COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses; COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Director Sharp:

Surescripts operates the nation's largest clinical health information network. Founded in 2001 by pharmacies and pharmacy benefit managers (PBMs) to enable electronic prescribing (e-prescribing), the company has moved beyond e-prescribing and today offers a wide portfolio of clinical messaging services. Surescripts services providers and patients in all 50 states and the District of Columbia and delivers over 700,000 clinical health transactions every hour. Every day more than 70 percent of all office-based providers use our services on behalf of over 3 million patients. We connect to over 99 percent of all retail pharmacies and most mail order pharmacies in the country, and we delivered over 1.91 billion prescriptions and 1.77 billion medication histories to providers this past year. Our provider directory contains over 1.61 million prescribers and our Master Patient Index covers 258 million insured lives. Surescripts has supported Maryland's efforts to increase the adoption of clinical exchange and privacy and security standards, through being recognized as a Registered Health Information Exchange (HIE) provider since 2016. Additionally, Surescripts has participated in several regulatory workgroups to advance the state's legislative efforts and has been recognized as an Electronic Health Network in Maryland via EHNAC accreditation for over 15 years. Additional information about Surescripts is available at www.surescripts.com, and we particular call your attention to our National Progress Report available at https://surescripts.widen.net/s/mvtqvvf5sd/2022-national-progress-report.

Below, we provide our responses to specific provisions to the proposed draft amendments:

I. COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses.

550 South Clark Street, Suite 1000
Arlington, VA 22202
T: 703.921.2121 F: 703.921.2191

900 2nd Avenue South, Suite 1300
Minneapolis, MN 55402
T: 866.267.9482 F: 651.855.3001

surescripts

a. ***.09(A)(4) – "The MHCC-certified EHN disclosed legally protected health information in violation of Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX".***

To be consistent with Health-General Article, §4-302.5, Annotated Code of Maryland, we recommend that "knowingly" be added as follows: "The MHCC-certified EHN ***knowingly*** disclosed legally protected health information in violation of Health-General Article, §4-302.5, Annotated Code of Maryland and COMAR XX.XX.XX".

We note that to be found guilty of violating §4-302.5, persons subject to this section must "knowingly" violate the section. Therefore, we think prior to any withdrawal of certification or issuance of penalties should require the Commission to clearly demonstrate that the person met the knowledge requisite. Otherwise, any withdrawal of certification or penalties issued to persons could be a result of a technical error or misunderstanding.

Furthermore, not all electronic health networks (EHNs) (e.g., health information network or exchanges) have the technical capability—nor is it their common practice—to peer into the transactions that cross their networks since they rely on their electronic health record or electronic medical record (EHR) customers to ensure that sensitive health information is not disclosed without appropriate patient authorization.

For all the reasons above, we respectfully request the Commission to add "knowingly" to the subsection.

b. ***.09(B)(2)(b) – "If a MHCC-certified EHN submits an implementation plan in accordance with §B(1), the EHN shall . . . Submit validation to the Commission by June 1, 2024 that it possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law."***

While we applaud the Commission's mission and goal to protect disclosure of legally protected health information, we believe the proposed requirement (1) does not appreciate alternative methods of achieving the same goals and (2) placed significant undue burden on EHNs.

First, as mentioned above, many EHNs rely on their EHR customers (and their health care providers) to ensure that sensitive health information is only disclosed with appropriate patient consent or authorization. For example, for its Record Locator & Exchange services, Surescripts provides its customers with policies and procedures that govern how patients must be educated about how their protected health information (including sensitive health information) will be maintained, used, and disclosed. Furthermore, the policies and procedures also govern how customers must provide patients with the ability to opt-out of disclosing their information (or revoke prior opt-out elections). Surescripts also incorporates such language into its customer services agreements.

550 South Clark Street, Suite 1000
Arlington, VA 22202
T: 703.921.2121 F: 703.921.2191

900 2nd Avenue South, Suite 1300
Minneapolis, MN 55402
T: 866.267.9482 F: 651.855.3001

We believe that this practice not only empowers patients to take control of their own information, but also ensures that needed medical treatment is not unnecessarily hindered due to technical defaults and additional administrative burdens placed on health care providers who are already inundated and burned out by the administrative tasks asked of them today. Surescripts has the vast experience and relationships with health care providers impacted by our services and network, to understand that sending inaccurate and incomplete health information to health care providers can lead to poor medical decisions and result in patient harm. Furthermore, many EHNs do not have the technical ability (nor a reason) to segment the health information being transacted across its network. Therefore, *all transactions* that happen to include legally protected health information, whether appropriately segmented or not, will require EHNs to notify their customers (EHR vendors or health care providers) that a patient's consent is needed. Undoubtedly, this will significantly increase the volume of transactions requiring additional patient consent, ad hoc, resulting in significant administrative burden on health care providers. If patient consent is not obtained and communicated to the EHN in an efficient manner, then we fear that this will become a bottle neck of access, exchange, and use of health care information and delay patients getting the needed treatment.

We note that pharmacies (and their technology vendors) have technical capabilities to adhere to patient opt-out and opt-in requests concerning data sharing, including the ability to suppress fill data they provide in accordance with state and local laws.

We also note that §4-302.5 does not explicitly require EHNs to adopt a technical solution to comply with the section.

Therefore, we respectfully recommend that the Commission allow flexibility to EHNs (especially if they are HIPAA and/or 42 C.F.R. Part 2 regulated entities) on how they comply with §4-302.5.

Second, even if the Commission disagrees that alternative methods can achieve the same result, as described above, we believe the technical requirement will place an undue burden on EHNs for the following reasons:

- Many EHNs merely provide transmission of information from one point to another point and do not have the technical capabilities to peer into the transactions crossing their networks. Neither is it their day-to-day practice to do so except for specific and authorized reasons requested by their customers (*i.e.*, troubleshooting, auditing purposes, investigations, etc.). In contrast, EHR vendors maintain patient information in their systems and have access to information maintained in their own systems. Therefore, because the proposed requirements undoubtedly require access to protected health information, it should place such requirements on those that already have access to such protected health information.
- Requiring EHNs to now have the capability of peering into transactions crossing its network places additional privacy and security responsibilities (and administrative

burdens) on those that have no purpose of accessing protected health information outside of this proposed amendment.

- If many EHNs simply transmit information from one point to another and do not maintain protected health information on their systems, then most likely they have no reason to segment information from other information. In contrast, most EHR vendors have the technical ability to segment certain types of information from other information so that they and their health care providers can comply with privacy regulations. Here, segmenting and filtering are probably synonymous with the proposed amendments. Therefore, any technical requirements to filter and restrict legally protected health information probably should be placed at the level of the EHR vendor before it even leaves the EHR vendor.
- Respectfully, we do not believe the Commission appreciates the significant costs, resources, and time to develop and implement a technical build required by this proposal. Asking EHNs to stop transactions to scan data will impact the reliability of information being shared and create technical challenges. For example, most clinical data is exchanged through electronic documents formatted following the Consolidated-Clinical Document Architecture (C-CDA). Within a C-CDA, data can be discreetly codified but does not necessarily have to be. Therefore, a technical solution to meet the requirements of the proposed amendment would require EHNs to analyze the C-CDA for both codified and free-text data while in transit for legally protected health care information. Stopping the transaction to perform this analysis will add costs to maintain the data in transit, will increase the likelihood of causing inaccurate or incomplete information, and will likely require industry engagement to identify proper procedures.

II. **COMAR 10.25.18, Health information Exchanges: Privacy and Security of Protected Health Information.**

We also would like the Commission to consider circumstances when the HIE or EHN is also a HIPAA regulated entity with roles and responsibilities as a Covered Entity or Business Associate especially regarding the interface with the individual health care consumer.

We request the Commission to clarify the intent and concerns giving rise to these proposed amendments so we could provide potential alternatives and language to meet the intent and concerns.

a. .04(C) – "Procedures for disclosing or re-disclosing legally protected health information."

Please see our comments and recommendations under I(b) of this letter.

We hope these comments and recommendations are helpful and thank you for the chance to participate in this process. Please contact us if you have any follow-up questions.

Best regards,

550 South Clark Street, Suite 1000
Arlington, VA 22202
T: 703.921.2121 F: 703.921.2191

900 2nd Avenue South, Suite 1300
Minneapolis, MN 55402
T: 866.267.9482 F: 651.855.3001

Justin McMartin
Manager Product Management
Surescripts
justin.mcmartin@surescripts.com

550 South Clark Street, Suite 1000
Arlington, VA 22202
T: 703.921.2121 F: 703.921.2191

900 2nd Avenue South, Suite 1300
Minneapolis, MN 55402
T: 866.267.9482 F: 651.855.3001

UNIVERSITY of MARYLAND MEDICAL SYSTEM

250 W. Pratt Street
24th Floor
Baltimore, Maryland 21201-6829
www.umms.org

CORPORATE OFFICE

October 4, 2023

VIA EMAIL
Ben Steffen
Executive Director
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, MD 21215
mhcc_regs.comment@maryland.gov

Re: *Proposed Emergency Regulation Amending COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information*
Informal Comments on behalf of the University of Maryland Medical System

Dear Mr. Steffen:

I write on behalf of the University of Maryland Medical System ("UMMS") to provide informal comments in response to MHCC's draft amendments to COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information* (the "Emergency Regulation"). UMMS appreciates the opportunity to provide informal comments on MHCC's proposed implementation of Chapter 249 (House Bill 812) Health – Reproductive Health Services – Protected Information and Insurance Requirements (the "Act"), and urges the Commission to adopt the Emergency Regulation while incorporating the revisions proposed in the comments herein.

UMMS supports the intended purpose of Chapter 249 without qualification. As a provider of abortion and other reproductive health services to many patients in Maryland every year, UMMS r ecognizes the pressing need to safeguard the confidentiality of medical records derived from this legally protected health care. To ensure this initiative is successful, UMMS joins other health care providers in proposing technical improvements to the Emergency Regulation in order to prevent potential unintended consequences detrimental to patient care.

COMMENTS ON SPECIFIC DRAFT AMENDMENTS TO COMAR 10.25.18

A. Definitions (10.25.18.02B)

10.25.18.02B(#) "Knowingly"

UMMS proposes that MHCC should define the intent element ("knowingly") for a violation of the Act to provide clear notice that violations of the statute require specific intent in order to incur civil and criminal penalties. The culpable party should only be subject to these penalties to the extent they know their actions violate the law. Accordingly, UMMS proposes that MHCC adopt the following definition:

10.25.18.02B

(##) "Knowingly" means a person, at the time of making a disclosure, has actual knowledge that legally protected health information is being disclosed through an HIE and that this disclosure violates Health-General Article § 4-302.5, Annotated Code of Maryland.

10.25.18.02B(40) "Legally protected health information"

UMMS proposes that the definition of "legally protected health information" should be refined in several respects to focus its application consistent with the intended scope of the Act.

First, the Act is silent as to what dates of service for legally protected health care its restrictions apply. Some may interpret this to be the effective date of the law, or the date upon which MHCC may begin to enforce the law in accordance with Health — General § 4-302.5(b). UMMS takes the position that MHCC's regulations should clarify that these protections apply to services provided on or after June 24, 2022, the date that the U.S Supreme Court decided *Dobbs v. Jackson Women's Health Organization,* No. 19-1392, 597 U.S. ___ (2022), which overruled *Roe v. Wade* and *Planned Parenthood v. Casey*, abrogating the Constitutional right to an abortion. The legislative intent of protecting recipients of legally protected health care, as well as providers of this care, from prosecution or other legal sanctions, is only served by application to that date forward. Of the states that immediately legally banned abortion via previously-enacted "trigger laws," these bans all applied on or after the date of issuance of the *Dobbs* decision. If the protections only begin to apply after the effective date of the law or later, an important subset of patients will be excluded from its protections. However, if data disclosure restrictions are applied further back in time than the *Dobbs*, these restrictions will impose unnecessary burdens on patient care without providing significant benefits in terms of protecting patients.

The definition of "legally protected health information" should also limit the geographic scope to relate only to health care provided in Maryland. This limitation is consistent with the geographic scope of MHCC's regulatory jurisdiction to the operations of HIEs in Maryland.

Finally, Mifepristone is used for medical purposes beyond abortion care, including miscarriage management and treatment of Cushing's syndrome. Accordingly, the restrictions on disclosure associated with Mifepristone should be narrowed to the prescription of Mifepristone for abortion care, consistent with the intent of the Act.

Consistent with the above comments, UMMS proposes that MHCC should amend this definition as follows:

10.25.18.02B(40)

(a) "Legally protected health information" means the health information subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including:

(1) Mifepristone data, as defined by the Secretary, prescribed after June 24, 2022 to a patient located in the state of Maryland related to the diagnosis of medical termination of pregnancy; and

(2) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes documented in structured data fields related to:

(i) Abortion care provided in the state of Maryland after June 24, 2022; and

(ii) Sensitive health services provided in the state of Maryland after June 24, 2022, as defined by Health-General, §4-301, Annotated Code of Maryland.

(b) "Legally protected health information" does not include an electronic prescription and prescription related information transmitted to a pharmacy of the patient's choice.

10.25.18.02B(##) "Specific treating provider"

The Act permits disclosures of legally protected health information through an HIE to "a specific treating provider" subject to the written consent of a patient or their parent or guardian. Md. Code, Health–General § 4-302.5(b)(2). "Specific treating provider" is not defined in the Act, and MHCC has not proposed a definition in the Emergency Regulation. To eliminate possible ambiguity in this term, and to give patients autonomy and control over disclosure of their legally protected health information, the Emergency Regulation should clarify that patients have the power to consent to disclosures of their own legally protected health information as they see fit and as serves their own needs to obtain health care. As such, MHCC should adopt a definition of "specific treating provider" consistent with that principal of patient autonomy and control, as follows:

10.25.18.04B

(##) "Specific treating provider" means a health care provider that a patient, or parent or guardian of a patient, gives consent to receive sensitive health information in accordance with COMAR 10.25.18.04.

B. Patient Consent to Disclosure (10.25.18)

10.25.18.03A*(5)* Right to Control Sensitive Health Information

Without MHCC action to clarify that health care consumers have the right to control their own sensitive health information, the Act will have the unintended effect of limiting consumer autonomy and choice as it relates to their participation in an HIE. The Emergency Regulation should make clear that the ultimate right to control sensitive health information is vested in patients themselves. MHCC should thus clarify that patients have the power to consent to disclosure of sensitive health information to any health care providers they choose, on a prospective basis, in anticipation of potential future treatment. This right will reduce the unintended consequence of denying patients the benefit of having any physician access their full medical record without facing an unnecessary administrative burden complete duplicative and redundant consent forms. As a consequence of enabling continued HIE participation, the following proposed regulation will enable providers to access information more efficiently and treat patients more effectively while maintaining the critical protective features of the Act. UMMS therefore urges MHCC to add the following regulation:

10.25.18.03A*(5)*

(5) The right to control sensitive health information, including the right to give written consent in advance to disclosure of legally protected health information to one or more health care providers with whom the health care consumer may have a future provider-patient relationship.

10.25.18.04A(2) Written Consent for Access, Use, or Disclosure of Sensitive Health Information

The Act permits disclosures of legally protected health information through an HIE to "a specific treating provider" subject to the written consent of a patient or their parent or guardian. Md. Code, Health–General § 4-302.5(b)(2) In addition to defining "specific treating provider," as proposed above, the MHCC must provide an interpretation of this consent process that provides health care providers, HIEs, and EHNs with sufficient notice as to what MHCC will enforce as appropriate parameters for obtaining that consent. Consistent with the principle that patient autonomy and control over their legally protected health information, MHCC should adopt a rule that gives patients the power to consent to disclosures as they see fit and as serves their own needs to obtain health care. UMMS proposes that the consent process should permit health care consumers to specify any providers they wish, notwithstanding a current treating relationship, for any duration of time, and with the right to revoke this consent upon reasonable notice. We urge MHCC to implement this rule as follows:

10.25.18.04B(2)

(2) If federal or State law requires written consent or authorization for access, use, or disclosure of sensitive health information, a person shall obtain consent or authorization consistent with the applicable law prior to the access, use, or disclosure of sensitive health information to and through an HIE to an authorized recipient, including as follows:

(a) A patient, or parent or guardian of a patient, providing written consent to a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may specify:

(i) Any health care provider to receive sensitive health information, at present or in the future, notwithstanding the existence of a current provider-patient relationship; and

(ii) The duration of the consent, up to and including an unlimited period of time.

(b) The consent obtained by a specific treating provider pursuant to Health-General Article, § 4-302.5(b)(2), Annotated Code of Maryland, may be revoked by the patient, or parent or guardian of a patient, at any time, upon reasonable notice.

Emergency Disclosures (10.25.18.04A(3))

The Act does not address emergency disclosures, and it is imperative that MHCC retain an emergency exception to ensure patients' critical information is available in an emergency. UMMS proposes that the following emergency exception replace the proposed amendment:

10.25.18.04A

(3) [Notwithstanding §A(2) of this regulation, an HIE may transmit sensitive health information, in accordance with state and federal law, 42 CFR § 2.51, and Health-General Article Title 4, Subtitle 3, Annotated Code of Maryland. [:

(a) To medical personnel who have a need for information about a patient for the purpose of treating a condition which poses an immediate threat to the health of any individual and which requires immediate medical intervention, as permitted by Part 2; and

(b) In an emergency, if a health care provider makes a professional determination that an immediate disclosure is necessary to provide for the emergency health care needs of a patient or recipient.] ~~*If federal or State law does not require written consent or authorization for access, use, or disclosure of sensitive health information a person shall not require consent or authorization prior to the access, use, or disclosure of the sensitive health information through an HIE.*~~

Enforcement (10.25.18.09(C)(3)(a))

The Act § 4-302.2(b)(iv) provides for "appropriate penalties for noncompliance with its HIE regulations, including fines that do not exceed $10,000 per day." The Emergency Regulation indicates that MHCC has chosen to adopt a rule that permits imposing civil penalties at a maximum of $10,000 per day "for each person impacted by the non-compliance." A fine imposed per day, per person, could exceed the statutory maximum of $10,000 per day, contrary to legislative intent. The regulations must also clarify that the civil penalties may be imposed only by the MHCC and with no private right of action. UMMS proposes the regulation be revised as follows:

(a) A person who knowingly fails to comply with this chapter shall be subject to a civil penalty imposed by the Commission not exceeding $10,000 per day ~~for each person impacted by the non-compliance~~ based on:

Thank you for your consideration of these comments. Please contact me with any questions.

Very truly yours,

Kristin Bryce

Kristin Jones Bryce
Senior Vice President and Chief External Affairs Officer
University of Maryland Medical System