MARYLAND
Health Care
Commission

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

Proposed Permanent Regulations: Stakeholder Comments in Response to Draft Amendments

April 18, 2024

(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: January 12th through February 12th 2024

Table of Contents

1. American College of Nurst-Midwives 4
2. Electronic Frontier Foundation 6
3. Epic 7
4. HIMSS Electronic Health Record Association (EHRA) 9
5. Kaiser Permanente 13
6. Maryland Hospital Association 17
7. National Women's Law Center 19
8. Oracle 21
9. Planned Parenthood of Maryland 27
10. Stevie Glaberson 28
11. Surescripts 29
12. University of California School of Law Center on Reproductive Health, Law, and Policy 39
13. Women's Law Center of Maryland 41
14. Provider 1 45
15. Provider 2 46
16. Provider 3 47
17. Provider 4 48
18. Provider 5 49

19. Provider 6 ..... **50**

20. Provider 7 ..... **51**

21. Provider 8 ..... **52**

22. Provider 9 ..... **53**

23. Provider 10 ..... **54**

24. Provider 11 ..... **55**

25. Provider 12 ..... **56**

26. Provider 13 ..... **57**

27. Provider 14 ..... **58**

28. Provider 15 ..... **59**

29. Provider 16 ..... **60**

30. Provider 17 ..... **61**

31. Provider 18 ..... **62**

32. Provider 19 ..... **63**

33. Provider 20 ..... **64**

34. Provider 21 ..... **65**

35. Provider 22 ..... **66**

36. Provider 23 ..... **67**

To: Anna Gribble
Program Manager
Maryland Health Care Commission

From: Robyn Elliott on behalf of the Women's Law Center of Maryland

RE: Proposed Regulations: 10.25.07 and 10.25.18

Date: February 12, 2024

Thank you for the opportunity to submit comments on the proposed regulations for *10.25.07* and 10.25.18 regarding electronic health networks (EHNs) and health information exchanges (HIEs). ACNM strongly supported SB 786/HB 812, which requires HIEs and EHNs to provide extra privacy protection for abortion records to prevent these records from being shared without the patient's consent. The Maryland Affiliate of the American College of Nurse-Midwives strongly supports the proposed regulations to implement this legislation. Without these regulations, Maryland patients and providers will be placed at great legal risk for the provision of abortion and other reproductive health care within our state borders.

On June 22, 2022, millions of Marylanders lost the fundamental right of bodily autonomy. With the *Dobbs* decision, the U.S. Supreme Court overturned *Roe v Wade* and eliminated constitutional protections for abortion rights. Justice Clarence Thomas also suggested that other protections, such as the right to birth control, may also be called into question.

Since the *Dobbs* decision, almost half of all states have enacted legislation to ban or severely restrict abortion access. These restrictive states, however, do not seem content to just stopping abortion within their states. Instead, they are adopting aggressive tactics to intimidate and even criminalize residents who travel out-of-state to seek abortion care. These tactics are creating a chilling effect on providers in states like Maryland. Abortion remains protected in our state, but our providers are frightened of attempts of restrictive states to impose criminal, civil, and administrative penalties.

Nurse-midwives, along with our physician and nurse practitioner colleagues, are struggling to provide reproductive health care to Marylanders and out-of-state patients alike. We are well aware that there have already been improper efforts to obtain records of reproductive records in other states.

We support the adoption of the proposed regulations in order to protect our patients, their families, and our Maryland colleagues who provide abortion care. If we can provide any additional information, please contact Robyn Elliott at relliott@policypartners.net.

February 8, 2024

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

Re: Request for Formal Public Comment, 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Ms. Gribble:

I write today on behalf of the Electronic Frontier Foundation, a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 30,000 active donors and members nationwide, including in Maryland. We commend Maryland for being the first state in the country to address the reproductive data privacy concerns posed by health information exchanges and express our support for the proposed regulations.

While EFF is not a reproductive rights advocacy group, our history of work on digital privacy—particularly health privacy—prompted us to raise concerns about the ways medical data are shared, particularly in the wake of the *Dobbs* decision. This proposal recognizes the real risks patients and medical care providers can face if health information is not protected and controlled in a thoughtful manner. It also rightly strives to provide patients with the information they need to make decisions about how to share their medical information. Health care requires trust between medical providers and patients. By establishing systems to notify patients, regularly audit systems, and safeguard information that could be extremely harmful in the wrong hands, Maryland will invest in the safety and security of people seeking abortion care, their providers, and personal support networks.

For these reasons, we support the proposed regulations. Thank you.

Sincerely,

Hayley Tsukayama
Associate Director of Legislative Activism
Electronic Frontier Foundation
(415) 436-9333 x 161

February 12, 2024

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

RE: Feedback on January 12, 2024, Publication of Maryland Register

Dear Executive Director Steffen and the Maryland Health Care Commission,

Thank you for the opportunity to share feedback on amendments 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. Epic is a developer of an electronic health record certified through ONC's program, and therefore Maryland considers us a health information exchange ("HIE") per these regulations and the definition of and HIE in Md. Code, Health-Gen. § 4-301(i)(1)(ii). We provide locally-deployed software to 58 different healthcare provider organizations that provide care in Maryland.

In each section, it is noted that the economic impact on regulated entities is unknown while expressing interest in better understanding this cost.

Epic estimates our effort as follows:

Epic Effort	Hours spent	Approximate cost of effort
Supporting our customers with implementing current tools to protect patient privacy (by restricting exchange of entire records) according to the October 2023 draft list of legally protected health care codes	2,000	$316,000
Updating from the October 2023 draft list of codes to the January 2024 list of legally protected health care codes	300	$44,000
Anticipated future effort each time the scope of sensitive health services or legally protected health care codes is updated	300-500 (depending on updates)	$44,000-74,000
Planned future development to permit customers to filter specific codes identified by the Maryland Department of Health from documents exchanged through Care Everywhere, our interoperability platform	1,400	$245,000
Supporting our customers with implementing the future development to filter specific codes from documents exchanged through Care Everywhere	500	$74,000

This estimate is not intended to be comprehensive, as we anticipate further effort will be needed based on subsequent regulatory updates. Notably, the estimates shown above do not reflect any work to meet expectations set in MHCC's January 2024 Technical Guidance document, which we anticipate needing further review and effort. Regardless, we hope our estimate here provides a basis for understanding the regulation's impact.

In addition, Epic estimates the following effort by our impacted customers:

Healthcare Organization Effort	Hours spent
Effort of 58 customer organizations to implement current tools to protect patient privacy, by restricting exchange of entire records, according to the October 2023 draft list of legally protected health care codes	1,160 (approx. 20 hrs per customer)
Effort of 58 customer organizations to update from the October 2023 draft list of codes to the January 2024 list of legally protected health care codes	400 (aprox. 7 hrs per customer)
Anticipated future effort of 58 customer organizations to implement each time the scope of sensitive health services or legally protected health care codes is updated	150-400 depending on updates (approx. 3-7 hrs per customer)
Anticipated future effort of 58 customer organizations to implement the planned future development	580 (approx. 10 hrs per customer)

To minimize the economic impact of any subsequent HIE regulation, we encourage all of the following:

1. Alignment with national standards for health information technology
2. Consultation with EHR developer technical experts prior to determining requirements and timelines
3. Setting deadlines appropriately to allow sufficient time for development, testing, and deployment of any new features

Thank you for your consideration,

Sasha TerMaat

EHRA
HIMSS ELECTRONIC HEALTH RECORD ASSOCIATION

350 North Orleans Street, Suite S10000
Chicago, IL 60654

@EHRAssociation | ehra.org

February 12, 2024

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

Jordan Green, Director
Office of Regulation and Policy Coordination
Maryland Department of Health
201 West Preston Street
Baltimore, MD 21201

RE: COMAR 10.11.18, COMAR 10.25.07 and 10.25.18

Dear Director Green and Executive Director Steffen,

The HIMSS Electronic Health Record (EHR) Association appreciates the opportunity to provide feedback on regulations published in January 2024:

> COMAR 10.11.18 (Abortion Care Disclosure)
>
> 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, our member companies support the vast majority of hospital, post-acute, specialty-specific, and ambulatory healthcare providers using EHRs and other health IT across the United States. Our shared purpose is to enhance care quality and efficiency through the adoption and utilization of innovative, interoperable, and secure health IT solutions.

Our previous communications, including the letter from October 2023, highlighted concerns regarding the new Maryland legislation requiring the filtering and segmentation of reproductive health information. These requirements definitively do not align with the existing capabilities of certified electronic health records in use in Maryland. Despite our efforts to clarify this through written communication, town hall discussions, and numerous phone conversations held with many of our member companies, the insufficient time originally outlined between the enactment of SB 0786 and the effective date for the development of new features has not been addressed. In fact, the scope of the work required by Maryland has significantly expanded, not decreased, in the Technical Guidance document released on January 12, 2024. This guidance unexpectedly extends the scope to include the segmentation of free text, which was explained clearly as functionality that the industry is entirely unprepared to deliver.

The EHR Association has routinely advised Federal and State regulators that a period of 18-24 months is necessary for the development of new EHR features once standards for that development have reached sufficient maturity for adoption. The additional few months following the December 1, 2023 deadline before penalties begin do not provide adequate time. Most importantly, data segmentation and consent technical standards necessary 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.

Additionally, certain added expectations in MHCC's Technical Guidance document may also be technically infeasible to implement with current technology. The EHR Association will follow up with more detailed feedback later in February.

COMAR 10.11.18

The COMAR 10.11.18 Summary of Economic Impact is correct in stating that "Currently, Electronic Health Networks (EHNs) and Health Information Exchanges (HIEs) do not have the ability to restrict certain health information from a patient's health records." We also agree that the cost of developing this mechanism is currently unknown. However, we are unfamiliar with the referenced Maryland Department of Health (MDH) discussions intended to estimate these costs.

EHR Association members are concerned about the assertion that the financial impact of these requirements on small businesses would be minimal. Given that the costs associated with this work will inevitably be transferred to healthcare providers in Maryland, including those in small practices operating as small businesses, it is unclear how this conclusion was reached. These providers will, in fact, experience an increase in their health IT costs due to this action.

Furthermore, it is important for the MDH to recognize that with each update to the sensitive data requiring segmentation, additional efforts will be necessitated from each EHN and HIE. This could lead to further cost increments with each update, impacting the overall financial burden on healthcare providers.

COMAR 10.25.07 & COMAR 10.25.18

The Summary of Economic Impact for COMAR 10.25.07 and COMAR 10.25.18 understate that entities "may incur costs when developing technology necessary to restrict…" data. Entities have already incurred expenses in analyzing Maryland's legislation and regulations, raising inquiries with the Maryland Health Care Commission (MHCC), and developing implementation plans. These costs will continue to accumulate as work continues.

The EHR Association strenuously disagrees with the MHCC assertions that "costs may be minimal" and that developers "could potentially leverage existing technology to implement the proposed regulatory requirements." As we have indicated in our previous letters, town hall meetings, and phone calls that individual companies have held with members of the MHCC staff, the technology to support Maryland's requirements does not yet exist. Further, the development of such technology is anticipated to take several years, imposing significant financial burdens on technology developers and the healthcare organizations in Maryland that they serve.

Appropriate Estimates

To develop an estimate, we refer you to the EHR Association's estimates of the effort to support similar patient-requested data segmentation requirements that were included in the ONC's 2023 HTI-1 Proposed Rule (see page 52). Developers estimated that over 100,000 hours per developer per product would be required to segment data as ONC proposed. While we recognize that the scope of HTI-1 is larger than that of SB 0786, the estimates provide insight into the massive amount of time and cost these types of data segmentation requirements can create.

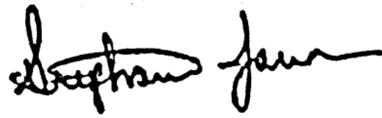
As explained above and in previous communications, the financial implications of implementing these requirements will be passed on to healthcare providers in Maryland, directly impacting small businesses, including physician practices and small hospitals, which already operate on razor-thin margins. The assertion that these actions will have a minimal impact on them is misleading.

Furthermore, MHCC should note that each time their guidance is updated, whether last-minute changes as in the Technical Guidance or other changes on any yet-to-be-announced regular cadence, estimated costs will need to be revised and are expected to increase.

The EHR Association has made numerous good-faith efforts to collaborate with the MHCC, beginning with a meeting request in January 2022 that was unfortunately declined. In the years since, our member companies have consistently voiced concerns about the technical infeasibility of certain proposals related to the segmentation and withholding of Protected Health Information. We implore the MHCC and MDH to meet with us, as the industry's trade association, for more viable approaches for the cost-effective implementation of SB 0786. The Association's leadership can be reached by contacting Kasey Nicholoff at knicholoff@ehra.org, who can help identify a time that will work for all stakeholders.

Thank you for your consideration.

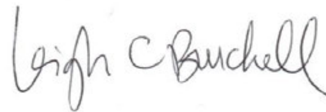
Sincerely,



Stephanie Jamison
Chair, EHR Association
Greenway Health

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

HIMSS EHR Association Executive Committee

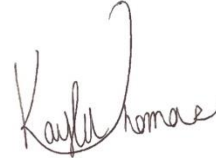


David J. Bucciferro
Foothold Technology

Leigh Burchell
Altera Digital Health

Danielle Friend
Epic

Cherie Holmes-Henry
NextGen Healthcare



Ida Mantashi
Modernizing Medicine

Kayla Thomas
Oracle Health

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

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

February 12, 2024

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

RE: Proposed Amendments for COMAR 10.25.18

Dear Mr. Steffen:

Kaiser Permanente appreciates the opportunity to comment on MHCC's proposed 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.

[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.

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, 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.

Implementation Plan

We appreciate MHCC's willingness to work with HIEs and health systems to ensure that HIEs possess the technological capability to 1) filter and restrict disclosure of legally protected health information to the extent required by law; 2) parse restricted codes and convey all other information that is not prohibited by law to exchange; and 3) allow a consumer to request and consent to the exchange of legally protected health information. In accordance with the meeting convened by the Health and Government Operations Committee on January 24, 2024, we request that MHCC not accept an HIE's implementation plan as compliant until all of the items above are satisfactorily met.

We understand that our vendor – Epic – plans to roll out a data parsing mechanism as part of its May 2024 system upgrade, that health systems may not be prepared to install by June 1, 2024. Many times, Epic will retrofit a code change (called a "system update") so that customers can install it on previous versions of their electronic health record as well, i.e., the version that is currently in effect. We request that Epic release this mechanism as a system update so that customers using a prior version can install it in a timely manner. To that end, we request that MHCC require, as part of an implementation plan, that an HIE to roll this out as a system update. To that end, we propose the following amendments:

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 10.11.08.

(2) By January 8, 2024, an HIE shall submit to the Commission:

(a) An affirmation that it:

(i) Possesses the technological capability to filter and restrict from disclosure legally protected health information to the extent required by law;

(ii) Is parsing restricted codes and conveying all other information in the health record that is not prohibited by law to exchange; ***[****and****]***

(iii) Possesses the technological capacity to allow a consumer to request and consent to the exchange of legally protected health information to a specific treating provider <u>*without limiting conveyance of all other information in the health record that is not prohibited by law to exchange; and*</u>

<u>*(iv) Has developed these technological capacities in a manner that is compatible with the technology versions used by its participating organizations, and will not create undue burden on participating organizations, such as requiring healthcare providers to create separate or additional documentation in order to achieve restrictions required by law*</u> *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 January 8, 2024, 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 of Health-General Article §4-302.5, Annotated Code of Maryland, 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) of this regulation, the HIE shall:

(a) Notify all participating organizations by January 8, 2024, that the HIE is unable to comply with §C(1) of this regulation 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.

Other Items

Kaiser Permanente notes that MHCC did not incorporate some items from our October 4, 2023 comment letter into the proposed regulations. We continue to advocate for these changes:

Scope

We propose clarifying 1) that mifepristone is in scope if prescribed for the purpose of "medical or surgical termination of pregnancy" (since it has other clinical applications), and 2) that the diagnosis, procedure, medication, and other codes are documented in structured data fields:

"Legally protected health information" means the health information with a date of service after May 31, 2022, that is subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, and COMAR 10.11.08, including:

(a) Mifepristone data, as defined by the Secretary, related to the diagnosis of medical or surgical termination of pregnancy; and

(b) As specified by the Secretary, the diagnosis, procedure, medication, and other codes documented in structured data fields related to:

(i) Abortion care; and

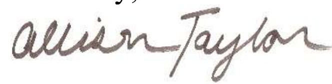
(ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.

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.

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

Sincerely,



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

Maryland
Hospital Association

February 12, 2024

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

Re: Comments on Proposed Amendments to COMAR 10.25.18

Dear Ms. Gribble:

On behalf of the Maryland Hospital Association's (MHA) member hospitals and health systems, we appreciate the opportunity to comment on the Maryland Health Care Commission's (MHCC) proposed amendments to COMAR 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information. These amendments effectuate House Bill (HB) 812, which was passed during the 2023 General Assembly legislative session to protect Maryland's reproductive health care providers and their patients—especially those from states that criminalize certain procedures that are permitted in Maryland.

MHA recognizes the importance of keeping our obstetricians, gynecologists, certified nurse midwives, labor and delivery nurses, and all other reproductive health providers safe from prosecution for performing services that comport with clinical standards of care. We appreciate the intent behind HB 812 and the amendments to COMAR 10.25.18, but we ask MHCC to ensure any information protections put in place by health information exchanges (HIE) do not impact patient safety or add administrative burdens on providers.

In the spirit of cooperation, we hope MHCC will serve as a transparent convenor for hospitals and HIE vendors to discuss the implementation of this law. We thank MHCC for its decision, as described in the *Implementation Guidance: Health Information Exchanges* (January 26, 2024), to make public all implementation plans submitted by HIE vendors. However, we ask MHCC to create a space for all HIE vendors working with hospitals and health systems to discuss any concerns going forward, especially as vendors begin operationalizing their implementation plans. Maryland hospitals are concerned with proposals from their electronic health records (EHR) vendors, which do not comport with the statutory requirements and jeopardize patient safety.

We appreciate MHCC's stance that "blocking records that contain legally protected health information [does not comply] with the intent of the law."[1] **We suggest also adding language to minimize clinician burden when designing the programs intended to protect health information and denying any implementation plans that require providers to take active steps during and/or after the patient visit.** For example, programs to separate protected health information should not require additional steps that detract from the clinician's face-to-face interaction with the patient (e.g., requiring the provider to open new programs, windows, or other interruptions to existing workflows). Any measures to specifically protect reproductive information should be performed automatically by the HIE.

We also ask MHCC to take the rolling nature of system updates into account when assessing the acceptability and operationalization of vendors' implementation plans. EHR systems often phase in system updates over a lengthy period. Even if hospitals have the same vendor, an update for one hospital that rolls out in June 2024 does not mean it is ready for operationalization at another hospital. Additionally, given the rushed timeline for vendors to create these new measures, any operational bugs or errors may need to be addressed before more widespread adoption in the hospital field. For these reasons, we hope MHCC will exercise regulatory discretion when assessing HIE (and indirectly, provider) compliance with the law.

We look forward to our continued partnership and collaboration on these regulations. Please contact me or my colleague Diana Hsu (dhsu@mhaonline.org) if you have any further questions or concerns.

Sincerely,

Erin M. Dorrien

Erin Dorrien
Vice President, Policy

---

[1] Maryland Health Care Commission. "Chapter 249/House Bill 812 (2023), Health – Reproductive Health Services – Protected Information and Insurance Requirements, Implementation Guidance: Health Information Exchanges." mhcc.maryland.gov/mhcc/pages/hit/hit_hie/documents/HIE_Guidance_012624.pdf (accessed February 12, 2024).

1350 I STREET NW
SUITE 700
WASHINGTON, DC 20005
202-588-5180
NWLC.ORG

February 12, 2024

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

Submitted Electronically

Attention: Comment in Support of the Implementation of HB 812/SB 786 with the proposed regulations

Dear Program Manager Gribble:

The National Women's Law Center ("NWLC") writes to comment in support of the implementation of HB 812/SB 786 with the proposed regulations.[1] NWLC fights for gender justice – in the courts, in public policy, and in our society – working across the issues that are central to the lives of women and girls, including child care and early learning, education, reproductive rights and health, income security, and workplace justice. We believe that access to reproductive health care, including abortion, is vital to gender justice. Everyone, no matter where they live, should have access to abortion care when they need it without barriers, fear, or stigma.

NWLC applauds Maryland advocates' and lawmakers' work in passing HB 812/SB 786, which bolsters privacy protections for medical records related to reproductive health information, the first law of its kind around the country. Following the erroneous decision in *Dobbs v. Jackson Women's Health Organization,*[2] where the U.S. Supreme Court overruled decades of precedent and declared there is no federal constitutional liberty right to abortion care, data privacy and surveillance concerns have heightened due to abortion bans that criminalize care taking effect across the country. The *Dobbs* decision exacerbated the already-existing patchwork of restrictive abortion laws and policies in the U.S. It intensified the ongoing legal and public health care crisis in scope and scale, causing increased fear and confusion among abortion providers, abortion seekers, and those who help them. This is exemplified in the recent surge in travel for abortion care around the country, largely caused by post-*Dobbs* abortion bans and restrictions.[3]

---

[1] Maryland Health Care Commission, Request for Formal Public Comment, https://mhcc.maryland.gov/mhcc/pages/home/public_comment/public_comment.aspx.
[2] *Dobbs v. Jackson Women's Health Org*., 142 S. Ct. 2228 (2022).
[3] Kimya Forouzan et. al., *The High Toll of US Abortion Bans: Nearly One in Five Patients Now Traveling Out of State for Abortion Care* (Dec. 7, 2023), https://www.guttmacher.org/2023/12/high-toll-us-abortion-bans-nearly-one-five-patients-now-traveling-out-state-abortion-care.

Maryland's bolstered privacy protections for reproductive health services records offer a model for states around the country that are looking for ways to increase protections for abortion seekers amidst the ongoing legal and public health care crisis. The new law ensures an abortion seeker's medical records are guarded and within the individual's own control. As we see a near-double increase in people traveling over state lines to seek abortion care in recent years,[4] privacy protections in states like Maryland—states that want to protect people's reproductive freedom—are all the more crucial. These guardrails can offer some needed protection and assurances of safety to people seeking abortion care in Maryland.

The National Women's Law Center appreciates the opportunity to comment in support of the implementation of HB 812/SB 786 and commends the work of advocates and lawmakers in Maryland. Over the years, Maryland has shown leadership in protecting people's reproductive freedom, and the passage of this law and its implementation is a part of that longstanding effort. For further information, please contact Sawyeh Esmaili, Senior Counsel at the National Women's Law Center at sesmaili@nwlc.org.

[4] "The latest study findings show that nearly one in five abortion patients traveled out of state to obtain abortion care in the first six months of 2023, compared with one in 10 abortion patients during a similar period in 2020." Guttmacher Institute, *New Data Show that Interstate Travel for Abortion Care in the United States Has Doubled Since 2020* (Dec. 7, 2023), https://www.guttmacher.org/2023/12/high-toll-us-abortion-bans-nearly-one-five-patients-now-traveling-out-state-abortion-care.

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

February 12, 2024

Dear Sir or Madam,

Oracle Health, a leading supplier of electronic health record, clinical and revenue cycle information systems, appreciates the opportunity to submit formal 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 amendments to COMAR 10.25.07 and COMAR 10.25.18. We are happy to help clarify any of the statements and appreciate the MHCC's consideration on this important matter.

Sincerely.

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

10.25.07.09.B & 10.25.18.04.C

An MHCC-certified EHN/HIE shall report on compliance progress to the Commission regarding possessing the technological capacity to allow a consumer to request and consent to the exchange of legally protected health information to a specific treating provider.

From Senate Bill 786 "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."

The current definition of 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. A patient's 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, Health 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.

Most regulations do not consider the need for better industry infrastructure that enables all the patient's data sources to evaluate all the applicable, up-to-date privacy, and consent rules whenever they are asked to share the data, or as they push out data to another party, using any means of interoperability (HL7 v2, HL7 C-CDA, HL7 FHIR, NCPDP, proprietary, etc.). 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 and accuracy through human error. Adding sensitivity flags based on data values is necessary but immediately introduces subjectivity.

The cleanest approach based on current functionality would be an opt out workflow. An opt out consent would be less burdensome and reduce risk of erroneous disclosures. It would also ensure all treating providers have the most up to date information available for clinical decision making. Providers would need to educate patients on the opt out consent process and provide direction for the patient to opt out.

Oracle provides the following recommendations.

1. Allow the exchange of legally protected health information to providers with a treatment relationship unless the patient as opted out of having this data shared.
2. If an opt out approach is not adopted, provide consent policy specifics:
    a. What fields must be captured with the consents.
        i. Additionally for Health IT vendors, identify if there are technical specifications to storing the consent.
    b. Guidance on when the consents should be captured.
    c. 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 health 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 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.

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 technology 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 a manual check 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 development from a 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.
    i. 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.
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) Increased risk of failure for a healthcare organization that do not have the minimum system or personal requirements in place. For the healthcare organization this could mean a loss in critical revenue, threat of data breaches, staff endangerment, and even patient safety events. 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.

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:

d) Staff training for the new process or technology (larger the organization, the more challenging it is to train all staff).

e) Device upgrades to ensure the adequate hardware is in place for the new process or technology.
f) Software upgrades to ensure that a new program is compatible with existing applications.
g) Facility upgrades to ensure that buildings and other physical infrastructure is in place for the change.
h) Command center coverage to make sure that there is a first response team in place for the actual cutover change time-period.
i) Front-line support to mitigate and address issues that occur during the change.
j) Ensuring there aren't overlapping conflicts/plans with other changes or major events that could result in the change not successfully taking hold.
    iii. 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.

10.25.07.09.B.1.a.ii & 10.25.18.04.C.2.ii

By January 8, 2024, an HIE shall submit to the Commission: An affirmation that it Is parsing restricted codes and conveying all other information in the health record that is not prohibited by law to exchange; and

HIT vendors are keenly aware of the need to continue to improve on data-level, patient-specific authorization capabilities, and continue to work on robust solutions for data segmentation. The development, the partner validation, and the overall release of this functionality by HIT vendors will not meet the stringent timelines set forth by Maryland. A rushed effort for new features being deployed to the market without adequate performance or functional testing is a high risk for error and inefficient processes. Appropriate time is needed for better data segmentation capabilities.

10.25.07.I & 10.25.18.I

Estimate of Economic Impact

The emergency regulations has the following statement "The cost of developing this technology is currently unknown; however, costs may be minimal as electronic health networks are accustomed to parsing and sorting health information and could potentially leverage existing technology to implement proposed regulatory requirements." Oracle health strongly disagrees with this assumption. As mentioned previously, there are numerous technologies and outbound channels for data transmission. To fully account for appropriate withholding or authorized transmission of abortion-related data, development is necessary for multiple products, data points and functionality for the intended consent capture/storage/check workflows. The development, partner validation, and the overall release of new functionality by HIT vendors can take up to 36 months. This requires significant engineering effort along

with likely consulting support for healthcare providers to adopt. We estimate costs between $2-3Million in development costs not accounting for implementation costs.

Technology is currently not developed yet that would allow unstructured text in notes to be identified and blocked from outbound transmission. Artificial Intelligence/Machine Learning capabilities are not ready to parse an unstructured note and identify sensitive elements with safe accuracy. This capability development will also have significant cost and engineering effort that has not been estimated yet.

Planned Parenthood®
Care. No matter what.

330 N. Howard Street
Baltimore, MD 21201
(410) 576-1400
www.plannedparenthood.org/maryland

Planned Parenthood of Maryland

To: Anna Gribble, Maryland Health Care Commission

From: Karen Nelson, CEO of Planned Parenthood of Maryland

Date: January 17, 2024

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

---

Planned Parenthood of Maryland (PPM) appreciates the opportunity to submit comments on the proposed regulation 10.25.18. PPM strongly supported the 2023 legislation that established the need for these regulations; we view the Maryland Health Care Commission as a critical partner in its implementation.

The electronic health records managed by health information exchanges (HIEs) are an integral part of our health care system. Exchanges have allowed providers to substantially improve coordination of care and health outcomes. However, since the summer of 2022 when the *Dobbs* decision reversed nearly 50 years of federal protection for abortion, electronic health record systems have become one of the most significant sources of risk for patients and providers. Prior to successful passage of *SB 786/HB 812 – Reproductive Health – Protected Information and Insurance Requirements* in 2023, laws did not adequately protect patients or providers from states seeking to criminalize or otherwise punish those receiving and providing abortion care. After the General Assembly overwhelmingly voted in support of the law, Maryland became one of the first states in the nation to mandate adequate privacy protection of patients' sensitive health data stored in electronic health records.

Without these proposed regulations, electronic health records and HIEs originally designed to improve health outcomes, pose a serious risk to both patients and abortion providers. As such, PPM is heartened to see these regulations and **supports** the requirements as proposed in 10.25.18.

Thank you for your consideration of our comments, and we look forward to working with the Commission to protect Maryland's patients and providers. If we can be of any further assistance, please contact Erin Bradley, Vice President of Public Affairs at erin.bradley@ppm.care.

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Comments in support of proposed regulations implementing HB 812/SB 786

1 message

Stevie Glaberson <Stephanie.Glaberson@georgetown.edu> Sat, Feb 10, 2024 at 9:29 PM
To: mhcc_regs.comment@maryland.gov

To: Anna Gribble, Program Manager, Maryland Health Care Commission

Please find below my comments in support of the implementation of HB 812/SB 786 with the proposed regulations, which I submit in my personal capacity:

I am a Maryland resident, a woman, a mother, an attorney and a researcher on data and privacy issues. I write to support the implementation of HB 812/SB 786 with the proposed regulations. As you know, while most people think their health records are protected under HIPAA, federal law currently allows for health records to be shared with any health care provider involved in a person's care. In fact, federal rules about electronic health records may be interpreted to require complete health records be shared with a person's other providers. While these rules may be positive for many patients, making it easier for healthcare providers to coordinate care, after the *Dobbs* decision, these rules now put abortion patients, their support networks, and their providers at risk. Thousands of people live in states that ban abortion. To seek abortion care, they are forced to travel to a safe state like Maryland. But they are only truly safe if their abortion health records remain within the safe state.

Maryland has sought to be a leader in protecting pregnant and birthing people in their rights to access all forms of medical care, and in the rights of gender nonconforming people to access gender affirming care. Those efforts could be undermined without the important protections HB 812/SB 786 and the implementing regulations provide. Even if people are able to access the care they need in Maryland, exposure of their medical records to care providers in care-hostile states could subject them to criminalization and family separation. Providers in hostile states may be mandated to report the occurrence of such care to authorities, or may simply choose to do so. As we have already seen, states hostile to abortion and trans rights are using not only their criminal legal apparatuses to target people seeking care and their families, but states, like Texas, also employ their "child protective" systems, threatening parents with separation from their children on the basis of their own health care decisions and those they think best for their children.

For all these reasons, I urge the Commission not only to adopt the currently-proposed regulations, but to continue work to ensure that all sensitive healthcare decisions people undertake in Maryland, such as to seek gender-affirming care for themselves or their children, is adequately protected.

STEVIE GLABERSON
Director of Research & Advocacy | she/her
Center on Privacy & Technology
Georgetown University Law Center
Ph: 202-662-9770

This communication may contain privileged and confidential attorney client information or attorney work product information Unauthorized disclosure or use of this communication is prohibited. If you have received this communication in error, please delete it and contact the sender immediately. Thank you.

Submitted via: mhcc_regs.comment@maryland.gov

February 12, 2024

Ms. Anna Gribble, Assistant Division Chief
Maryland Health Care MHCC
4160 Patterson Avenue
Baltimore, MD 21215

RE: Notices of Proposed Action: 10.25.07 Certification of Electronic Health Networks and Medical Care Electronic Claims and 10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information

Dear Ms. Gribble:

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. As a Registered HIE, Surescripts provides its Record Locator & Exchange and Clinical Direct Messaging services, which exchanged over forty-two million (42M) clinical documents in 2023 to treat patients in Maryland. Additionally, as a Certified Electronic Health Network ("EHN") provider, more than fifty-nine thousand (59,000) providers utilized Surescripts' medication history solution. Moreover, 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. Further 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.

We appreciate the opportunity to submit our comments to the Maryland Health Care MHCC's (MHCC's) proposed regulations. We are also encouraged by MHCC's efforts to protect the sensitive health information of its residents. However, we believe that some of the proposed changes to the regulations will have significant unintended effects that perhaps the MHCC has not appreciated. We urge MHCC to take into consideration our responses below and work with

industry experts to ensure we achieve Maryland's intent while minimizing the impact of its new regulations on health care providers' and patients' access to necessary health care information. Below, we provide our responses to specific provisions to the proposed amendments:

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

a. The Economic Impact of COMAR 10.25.07 Will Be Significant.

Respectfully, we disagree with the Estimate of Economic Impact found in the proposed action and do not believe MHCC 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 and timeliness 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 stakeholder engagement to ensure interoperability and conformity across different health IT systems, let alone compliance with a myriad of federal and state laws.

We estimate that the development, implementation, and support of the filtering codes from C-CDAs would require EHNs (e.g., Surescripts) to expend at least $5 million to $7 million dollars. The added network services would be an additional annual cost of at least $300,000 to $500,000 performing the filtering. These numbers are minimums based on the assumed filtering of codes. Additional costs would very likely apply to filtering free-text notes from C-CDAs because there are significant unknowns in how to approach this type of filtering to prevent harm to a patient.

b. .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".

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"**.

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 MHCC should be required 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 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 (EHR) or electronic medical record (EMR) customers to ensure that sensitive health information is not disclosed without appropriate patient authorization.

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

c. ***.09(A)(5) – "The MHCC-certified EHN violated a provision of COMAR 10.25.18.***

Similar to our comment above**, we recommend that "knowingly" be added as follows**: **"The MHCC-certified EHN *knowingly* violated a provision of COMAR 10.25.18."**

d. ***.09(B)(1)(a) – "An affirmation that to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland, it:***
   i. ***Possess the technological capability to filter and restrict from disclosure legally protected health information;***
   ii. ***Is parsing restricted codes and conveying all other information in the health record that is not prohibited by law to exchange; and***
   iii. ***Possesses the technological capacity to allow a consumer to request and consent to the exchange of legally protected health information to a specific treating provider"***

While we applaud the MHCC's mission and goal to protect disclosure of legally protected health information, we believe the proposed requirement (1) is a gross misinterpretation of Maryland statute, (2) does not consider less intrusive alternative methods of achieving the same goals, and (3) unnecessarily places significant undue burden on EHNs.

First, we note that *Health-General Article, §4-302.5, Annotated Code of Maryland* does not explicitly require EHNs to adopt a technical solution to comply with the section. In fact, while §4-302.5 states that "a health information exchange or electronic health network may not disclose Mifepristone data or the diagnosis, procedure, medication, or related codes for abortion care and other sensitive health services" it is silent on how that is to be achieved. Respectfully, we believe the proposed language at COMAR 10.25.18.09(B)(1)(a) incorrectly implies that *Health-General Article, §4-302.5, Annotated Code of Maryland* requires EHNs to have the technological capabilities described in this subsection when it does not prescribe it.

Second, as mentioned earlier, many EHNs rely on their EHR customers (and their health care provider end users) 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, these 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.

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 insight around the concerns of 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 transmitted 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 a 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 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 prescription dispensing data they provide in accordance with state and local laws.

Therefore, we respectfully recommend that the MHCC 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.

Third, even if the MHCC disagrees that alternative methods can achieve the same result, as mentioned above, we believe the technical requirement will place an undue burden (financially and developmentally) on EHNs for the following reasons:

i. Concerning the requirement: "Possess the technological capability to filter and restrict from disclosure legally protected health information":

- Many EHN technologies, including that employed by Surescripts, simply connect two or more individuals or entities to facilitate the exchange of information in real time. As the exchange occurs, these EHNs facilitate connectivity and trust among the parties but do not access or review the clinical information exchanged. Therefore, such EHNs are limited in what they can provide in response to subpoenas requesting sensitive health information. However, this law and related proposed regulations would require these

EHNs to possess knowledge of specific patient sensitive health information, which then would require them to disclose in response to subpoenas (court-ordered, law enforcement, or otherwise) as applicable to federal and state privacy laws. We believe this would be contrary to the legislative intent behind COMAR 10.25.07 and *Health-General Article, §4-302.5, Annotated Code of Maryland* and should therefore be avoided.

- Requiring EHNs to implement a technical solution would be infeasible because it would require wholesale network changes that do not align with the operations of national trust frameworks. For example, DirectTrust Standards for Direct Secure Messaging limit the ability of a network to peer into the content of clinical messages.

- Requiring EHNs like Surescripts to develop the technology to hold clinical data in transit for the purposes of reviewing and filtering of particular information from more than one (1) billion transactions annually to occur at the network level is impractical because it would add millions of dollars in operating costs. The added complexity of developing such technology will invariably translate to higher costs to operate the Health Information Exchange services in Maryland. This will most likely make it infeasible to continue providing the EHN services to Maryland customers at a reasonable cost.

ii. Concerning the requirement: "parsing restricted codes and conveying all other information in the health record that is not prohibited by law to exchange":

- We note that not all EHNs or HIEs are the same. Some EHNs simply transmit information from one point to another and do not maintain protected health information on their systems (e.g., Surescripts) in a designated record set or otherwise. Therefore, most likely they have no reason to segment information from other information. This law and related proposed regulations implicitly would require EHNs to unnecessarily create and maintain patient health records or designated record sets (as defined in HIPAA) since developing a technical capability to parse or segment fragmented data outside a designated record set would be quite infeasible and nonsensical. For example, to parse or segment data without a designated record set or patient record system, EHNs would be required to capture every variation, synonym, reference to a whole host of terms and phrases surrounding reproductive health, abortion-related items and services, gender-affirming care, and the like (yet somehow distinguish those that may overlap with other non-sensitive health items and services), which would be nearly impossible. Therefore, the proposed law would inevitably require EHNs or HIEs that do not maintain patient records or designated record sets to do so, increasing not only costs but unnecessarily placing various legal (federal and state) responsibilities and liabilities on those EHNs and HIEs.

- But even if EHNs possessed designated record sets or maintained data according to patient records, many EHNs and HIEs do not have the technical capability to segment certain sensitive health information from other health information. This was foreseen by

the Office of National Coordinator of Health IT (ONC) when it created the Privacy and Infeasibility exceptions. In preamble guidance, ONC explicitly states that "an actor is not required to fulfill a request for access, exchange, or use of EHI *if the actor cannot unambiguously segment the requested EHI from other EHI: (1) Because of a patient's preference or because the EHI cannot be made available by law*" (emphasis added) 85 Fed. Reg. 25642, 25867 (May 1, 2020). Therefore, without a feasible way to parse and segment data, the Maryland proposed law would inevitably cause an "all or none" approach in which EHNs would not be permitted to provide access, exchange, or use of any patient data because of the risk that legally protected health information would be disclosed in conjunction with non-legally protected health information.

But because we acknowledge that other EHNs may maintain protected health information on their systems, we request that any requirements (e.g., parsing or segmentation) be required for those EHNs that maintain electronic protected health information in a designated record set (as defined in HIPAA).

iii. <u>Concerning the requirement: "Possesses the technological capacity to allow a consumer to request and consent to the exchange of legally protected health information to a specific treating provider":</u>

- Many EHNs most likely address compliance with patient consent and authorization laws through role specification in their Business Associate Agreements (BAAs) in accordance with the HIPAA Privacy Rule. Furthermore, the HIPAA Privacy Rule does not require patient consent or authorization for "treatment, payment, and healthcare operations" purposes (as defined under HIPAA). And because EHNs generally facilitate exchange of protected health information (including legally protected health information) for only treatment or healthcare operations purposes, many EHNs have not needed to develop or acquire technologies to obtain, maintain, and distribute patient consents, let alone requests. Some EHNs are strictly business-to-business (e.g., Surescripts) and therefore have no direct interactions with patients. Therefore, such EHNs place patient consent or authorization requirements on their customers (many of them Covered Entities) since those customers are patient facing and are readily positioned to obtain the necessary consents or authorizations.

- Furthermore, no mature, nationally recognized, or widely adopted health information technology standards exist today for capturing consent at a granular data element level. Until they do, it would be premature to develop a solution that could result in non-interoperable standards and implementation specifications. The ONC recognized this complex issue and the need to solve for it when it decided not to finalize the adoption of a new criterion under its Privacy and Security Framework to support additional tools for implementing patient requested privacy restrictions around uses or disclosures of data in its most recent final rule (HTI-1). ONC's reason included "concerns about feasibility, timelines, and the overall complexity of the workflows" expressed by ONC and many commenters. Furthermore, ONC noted that "there was no clear consensus on whether and

how to proceed either with immature and untested standards or without the required use of specific standards", agreeing "with the concerns on the high risk of "wide variety of misaligned standards and implementation specifications, as well as increased burden on developers of certified health IT, health care providers, health information exchange networks, and a high probability of confusion for patients." 89 Fed. Reg. 1192, 1301 (Jan. 9, 2024).

Therefore, if MHCC requires EHNs to meet this technical requirement, **we request MHCC to provide the standards and specifications to ensure interoperability among all stakeholders that will be affected (including but not limited to EHNs, HIEs, EHRs/EMRs, and other health IT developers).**

e. ***.09(B)(2)(b) – "Submit validation to the MHCC 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.***

Even if a technological build required by the proposal were feasible, the very short timeline (eight [8] months from the date proposed amendments were made publicly available to implementation deadline) to develop and implement the required technologies is not reasonable. **We recommend an approach where clear standards for exchange, filtering, and consent are defined and a timeline of at least eighteen (18) months to implement those standards would make compliance possible for most EHN and HIE services.**

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

We also would like MHCC 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 MHCC 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. The Economic Impact of COMAR 10.25.18 Will Be Significant.

Similar to the reasons shared in Section I(a) of this letter, we disagree with the Estimate of Economic Impact found in the proposed action and do not believe MHCC appreciates the significant costs, resources, and time to develop and implement a technical build required by this proposal.

As we attempt to explain in Section I(d)(iii) of this letter, there are no nationally recognized or industry-adopted standards and implementation specifications to capture patient consent and authorizations at the granular level that MHCC has proposed because it is a very technical and complicated matter. Therefore, we foresee that the technical requirements outlined by the

regulations will probably require HIEs (e.g., Surescripts) to make significant changes to their core infrastructure network systems. First, the patient's consent needs to be exchanged among the network and accessible to each HIE. Under the current requirements, a bespoke system would need to be defined and implemented by each HIE. Second, members of each respective HIE network would be required to capture and exchange the consent through the bespoke solution across impacted products. Third, HIEs would need to implement a solution to begin monitoring all patient transactions to use the captured consent as transactions are processed. Fourth, HIEs would need to implement the filtering solution to remove the unconsented to information in the message. Finally, HIEs would need to audit the removal of data to ensure the actions taken on the network are safe and follow the requirements and wishes of the patient.

Given our twenty-plus years of experience in the industry, we estimate that engaging in this bespoke and complex type of effort would cost multi-millions of dollars. Today, hundreds of Surescripts customers would be impacted including provider offices, health systems, and electronic health record vendors. These customers would be impacted with costs to implement. Additionally, thousands of providers will need to incorporate workflows to utilize the updated consent tracking and filtering. Until MHCC (or another standards organization) prescribes a standard and implementation specifications, it will be difficult to estimate costs to developing and implementing such a solution.

b. .01(B)(1)(b) – "A health information technology developer of certified health information technology as that term is defined in Regulation .02B(33) of this chapter"

Our interpretation of .01(B)(1) appears to narrow the definition of HIE to those that meet subsections (a) and (b). We note that this would exclude HIEs that are not health IT developers of certified health IT. **We request MHCC to clarify if this is the intended effect and the purpose of it.**

c. .01(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 .09G or H of this chapter."

We applaud MHCC's recognition that HIEs may not feasibly be able to comply with the technical specifications required under this law and related proposed regulations and therefore allows HIEs to satisfy them via other methods. **First, we request that similar exemptions also be added to COMAR 10.25.07.**

Second, we note that in MHCC's "Implementation Guidance: Health Information Exchanges" (Jan. 26, 2024), MHCC states that "HIE's should execute written agreements by June 1, 2024 to avoid blocking all records that contain legally protected health information as a result of a client's decision to delay implementing an HIEs technical solution." **We seek clarity on how HIEs are expected to utilize COMAR 10.25.18.09G as a means to comply with the law and related proposed regulations if its clients either refuse to implement or do not execute a**

written agreement by the June 1, 2024 deadline. In other words, if HIEs attempt to satisfy COMAR 10.25.18.09G by executing written agreements with its participating organizations but certain participating organizations either refuse or delay in executing written agreements, how should those HIEs respond? It is unclear from the MHCC's guidance whether those HIEs are permitted to terminate or suspend services to the participating organizations that refuse or delay executing written agreements by June 1, 2024.

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

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

e. ***.09(G) – "If an HIE has reasonably determined that it is unable to independently meet any requirements of this chapter, then the HIE shall develop and implement policies to ensure the HIE's compliance through the execution of a written agreement with a participating organization or a business associate that will bring the HIE into compliance with this chapter. Every year as a part of the registration renewal process, the HIE shall submit a written attestation by an independent third-party auditor to the MHCC, attesting that the HIE has been in full compliance with the requirements of this chapter for the 12-month period prior to the audit."***

If HIEs choose to comply with this section**, we seek clarity of the following:**

III. What types of independent third-party auditors are acceptable to MHCC? What types of auditors perform such audits specific to the proposed regulations prescribed therein?

IV. What would auditors be auditing? Policies, procedures, written agreements? What would they be specifically looking for?

In order for HIEs to consider whether compliance with COMAR 10.25.18.09(G) is even an option, MHCC should specify its expectations. Until it does, MHCC should not expect HIEs to comply by June 1, 2024 and should **consider delaying the deadline until at least one (1) year after it publishes those expectations**.

V. Additional Comments

We would like to reiterate that we use and disclose PHI as a HIPAA Business Associate and follow HIPAA Privacy Rules in terms of disclosure to law enforcement agents that permits, *but does not require*, certain disclosures to law enforcement and others, subject to specific conditions. We also note that the Office of Civil Rights' (OCR's) Notice of Proposed Rulemaking (NPRM) (April 12, 2023) is intended to strengthen the protection of sensitive information related to reproductive health care and bolster patient-provider confidentiality, which would include the prohibition of use or disclosure of PHI for purposes of:

- A criminal, civil, or administrative investigation into or proceeding against any person in connection with, seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided; and
- The identification of any person for the purpose of initiating such investigations or proceedings.

We believe that once OCR's Privacy Rule is finalized, HIEs and EHNs will be able to work with health care providers (and their EHR vendors) to protect legally protected health information with the same effect and desired result intended by Maryland lawmakers and MHCC.

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.

Sincerely,

Daniel Kim, Esq.
Senior Regulatory Counsel
Surescripts, LLC

February 12, 2024

Anna Gribble
Program Manager
Maryland Health Care Commission
4160 Patterson Avenue
Baltimore, Maryland 21215
mhcc_regs.comment@maryland.gov

Re: Support for Proposed Regulations Implementing HB 812/SB 786

Dear Ms. Gribble:

We respectfully submit these comments to support implementation of HB 812/SB 786 by amending regulations under COMAR 10.25.07, Certification of Electronic Health Network and Medical Care Electronic Claims Databases, and COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information.

Maryland has become a safe haven for individuals living in states that ban abortion. Yet, as patients travel to Maryland to receive abortion care, there is a real risk that—if the state's medical record privacy protections are not adequately implemented—information related to care provided in Maryland could be accessed and used by law enforcement and private actors in states with bans to institute criminal, civil, and disciplinary actions against providers and patients.

Federal laws and regulations about medical records do not yet sufficiently protect patients or providers in our newly criminalized environment. Currently, federal law essentially requires sharing of health information across state lines through electronic health records systems and health information exchanges (HIE). This means that a patient's medical records about an out-of-state abortion are generally accessible by their home-state providers. The home state provider's access to this information could pose a substantial threat: the home state provider may be subject to record demands, and a recent study found that the most common way pregnant people are criminalized is through a report to law enforcement from a healthcare provider.[1] Possible federal regulatory change is in progress but current proposed rule changes do not go far enough to completely protect abortion patients and providers.[2]

Seeking to plug this significant hole in federal protections, Maryland's HB 812/SB 786 prohibits HIE disclosure of information related to abortion care without express patient consent and requires HIE and electronic health networks (EHN) to redesign their systems to protect such

[1] Laura Huss, Farah Diaz-Tello, and Goleen Samari, *Self Care, Criminalized: The Criminalization of Self Managed Abortion from 2000 to 2020*, If/When/How: Lawyering for Reproductive Justice (2023), available at: https://www.ifwhenhow.org/wp-content/uploads/2023/10/Self-Care-Criminalized-2023-Report.pdf.

[2] Indeed, the federal government recently passed up an opportunity to protect abortion data from being shared across state lines in new rules about electronic health records issued by the Department of Health and Human Services Office of the National Coordinator for Health Information Technology. 45 C.F.R. §§ 170, 171 (2024).

data. This is a groundbreaking and necessary stopgap measure to prevent electronic health record systems from jeopardizing the safety and security of healthcare providers and people seeking abortion care. Although several states are working towards enacting similar protections, California is currently the only other state that has passed a similar law. The many other states seeking to protect their citizens and those traveling to their states for abortion care are looking to Maryland and California as exemplars.

It is thus crucial that Maryland enact regulations to effectively implement its privacy protections. The proposed regulations, which provide enforcement mechanisms to ensure EHN and HIE compliance, are necessary to make the state's privacy protections meaningful. As we work towards redesigning health information systems to protect people seeking and providing abortion and other sensitive health care services, Maryland should continue to be a leader in changing the national landscape by adopting the proposed regulations.

Respectfully,

Melissa Goodman
Executive Director
Center on Reproductive Health, Law, and Policy
UCLA School of Law
goodmanm@law.ucla.edu

Amanda Barrow
Senior Staff Attorney
Center on Reproductive Health, Law, and Policy
UCLA School of Law
barrowa@law.ucla.edu

Women's Law Center of Maryland
JUSTICE FAIRNESS EQUALITY
102 West Pennsylvania Avenue, Suite 100 Towson, MD 21204
phone 410-321-8761 fax 410-321-0462 www.wlcmd.org

To: Anna Gribble
Program Manager
Maryland Health Care Commission

From: Robyn Elliott on behalf of the Women's Law Center of Maryland

RE: Proposed Regulations: 10.25.07 and 10.25.18

Date: February 12, 2024

Thank you for the opportunity to submit comments on the proposed regulations for *10.25.07* and 10.25.18 regarding electronic health networks (EHNs) and health information exchanges (HIEs). The Women's Law Center of Maryland supports the proposed regulations and appreciates the Maryland Health Care Commission's commitment to implementation of the provisions of *House Bill 812/Senate Bill 786 - Health - Reproductive Health Services - Protected Information and Insurance Requirements* of the 2023 Session. When enacted by the Maryland General Assembly and signed into law by Governor Moore, Maryland became the first state to provide specific privacy protections for electronic health records related to abortion care. These protections are essential, as many out-of-state individuals are seeking abortion care in Maryland because almost two dozen states have enacted abortion bans.

Protecting out-of-state individuals seeking abortion care, their support networks, and their Maryland providers

When individuals are forced to travel out-of-state for abortion care, it is absolutely essentially that their health records about abortion care stay within Maryland. Otherwise, there is great risk of civil, administrative, and even criminal penalties for the individuals obtaining abortion care, their providers, and their support networks, including friends and family that supported them in traveling for abortion care. However, health information exchanges and electronic health networks routinely link the health records of Maryland providers with the individual's other health care providers. As a result, the health record of an abortion occurring in Maryland is integrated into the electronic health records of nearly all of an individual's treating providers in their home state.

Maryland has enacted shielding laws that prevent information and records about abortion care being discoverable in a criminal, civil, or administrative proceedings initiated because the patient lives in a state that bans abortion. However, our laws only protect the electronic health records maintained by Maryland providers. If a patient lives in a state that bans abortion, the patient, along with their provider and any people who supported them in obtaining abortion care, are at risk because of the interoperability of electronic health records. It is possible to obtain a record about an abortion in

Maryland through a subpoena to one of the patient's providers in their home state. Anyone with legal standing, which includes private individuals under SB 8 in Texas, may be able to obtain the record of abortion care through a subpoena or other legal instrument to a patient's home state provider. Through implementation of HB 812/SB 786, the Commission is ensuring the safety of anyone who needs to seek abortion care in Maryland, their support networks, and their Maryland abortion providers. This law is critical in making Maryland a safe state for all who seek reproductive health care within our borders.

Protecting abortion providers by ensuring the privacy of mifepristone records

The Commission's proposed regulations implement critical protections of mifepristone records, ensuring that the identity of abortion providers remains protected. This provision protects the safety of Maryland abortion providers. By doing so, it will also protect access to abortion care in Maryland. If abortion providers face the risk for being identified, many of them will be too afraid to provide abortion care.

Right now, vendors routinely collect pharmacy dispensing data, including the prescriber's name, to be integrated into electronic health records. In the past, the practice of disseminating prescription dispensing data did not pose a risk to abortion providers. Mifepristone, the primary medication used in medication abortion, could not be dispensed by pharmacies because of a federal rule. Providers had to dispense the medication in their offices. However, the Food and Drug Administration changed this rule in December 2022, and prescribers may send Mifepristone prescriptions to pharmacies, just as with any other medication. This rule change has the potential to significantly improve access in underserved areas. However, it does mean that information about Mifepristone, including the prescriber's name, could soon be widely integrated into electronic health records in Maryland and across the country. This practice means that abortion providers face an exponentially higher risk of being identified – risking their employment if their health facilities do not support abortion. And even worse, abortion providers, their staff, and their families face a heightened risk of violence.

This risk is not theoretical. It is real and long-standing, existing since Mifepristone was first developed. There are long-standing practices of protecting providers and people affiliated with Mifepristone. In *Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 153 (D.C. Cir. 2006), [i] the U.S. Court of Appeals heard a case about the Food and Drug Administration's policy of redacting identifying information under a freedom of information request for the names of the individuals involved in the review of the application for approval for Mifepristone. The Court found that:

> *" (the FDA has) fairly asserted abortion-related violence as a privacy interest for both the names and addresses of persons and businesses associated with mifepristone."*
>
> In making this determination, the Court cited that,

“As its privacy interest, the FDA cited the danger of abortion-related violence to those who developed mifepristone, worked on its FDA approval, and continue to manufacture the drug. The supporting affidavits detail evidence of abortion clinic bombings. They also describe websites that encourage readers to look for mifepristone's manufacturing locations and then kill or kidnap employees once found. Based on these declarations, the FDA fairly asserted abortion-related violence as a privacy interest for both the names and addresses of persons and businesses associated with mifepristone. “

Through implementation of the proposed regulations for HB 812/SB 786, the Commission will protect access to abortion care in Maryland by protecting the identify of abortion providers.

Conclusion

The Women’s Law Center of Maryland greatly appreciates the Commission’s collaborative approach to the development and implementation of the proposed regulations. Since Maryland is the first state to implement specific privacy protections of electronic health records for abortion care, there has not always been a clear roadmap for implementation. However, the Commission has persevered; and through collaboration with partners from consumer, health information technology, and health provider perspectives, the Commission has forged a path forward. The proposed regulations provide vendors with the flexibility needed to implement the law’s new privacy protections and create a blueprint for other states to follow. California has already enacted similar legislation, and New York may follow with the introduction of a bill this month.

Please let us know how the Women’s Law Center of Maryland can continue to support the Department of Health in the implementation process. If you need any additional information or resources, please contact Robyn Elliott at relliott@policypartners.net.

The Women’s Law Center of Maryland is a private, non-profit, legal services organization that serves as a leading voice for justice and fairness for women. It advocates for the rights of women through legal assistance to individuals and strategic initiatives to achieve systemic change, working to ensure physical safety, economic security, and bodily autonomy for women in Maryland.

[i] *Judicial Watch, Inc. v. Food & Drug Admin.*, 449 F.3d 141, 153 (D.C. Cir. 2006)

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support of HB 812/SB 786

1 message

Mon, Feb 12, 2024 at 12:09 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

I work in New York but have lived in many other states (Virginia, Texas, Connecticut) with varying laws and have many loved ones who reside in Maryland currently. As a volunteer for the miscarriage and abortion hotline, I regularly hear patients' concerns that someone will find out that they have had an abortion in another state. I want to reassure them that won't happen but I can't because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients' in the setting of abortion, it means that those patients miss out on the ability of providers to see records from specialty, radiology, or hospital visits,

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can't wait!

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Protect patient data re: abortions

1 message

Sun, Feb 11, 2024 at 10:16 AM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a when I provide information for people seeking information about miscarriage and abortiion, I have heard patients' concerns that someone will flnd out that they have had an abortion in another state. I want to reassure them that wont happen but I can’t because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients’ in the setting of abortion, it means that those patients miss out on the ability of providers to see records from specialty, radiology, or hospital visits,

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can’t wait!

I urge the implementation of HB 812/SB 786.

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support for Privacy Law in Healthcare

1 message

Sun, Feb 11, 2024 at 8:15 AM

To: mhcc_regs.comment@maryland.gov

Hello,

My name is [redacted], and I am a family physician and abortion provider in [redacted].

I wanted to write this morning and express my support for upholding the privacy law for abortion patients. Ensuring the privacy of patients seeking abortion is critical, especially for my practice, as we are often referring patients out of state to places like Maryland.

Thanks for your time,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

HB 812/SB 786

1 message

Sun, Feb 11, 2024 at 7:25 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission,

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a volunteer for the miscarriage and abortion hotline, I regularly hear patients' concerns that someone will find out that they have had an abortion in another state. I want to reassure them that wont happen but I can't because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can't wait! Thank you.

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Testimony in support of HB 812/SB 786

1 message

Sun, Feb 11, 2024 at 7:20 AM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

When I was training in abortion care in Minnesota, I regularly heard patients' concerns that someone would find out that they have had an abortion in another state. I wanted to reassure them, but because I know that some medical records, including abortion records, are easily discoverable and could be used to criminalize them, as healthcare providers are a common reporter of abortion care to law enforcement.

Now, as a provider of both abortion care and prenatal care on the East Coast, I have referred several patients to clinics in Maryland for abortion care. To have the additional reassurance that my patients' abortion records will be secure makes me more confident in doing so.

Please support HB 812/SB 786- we can't wait!

Sent from my iPhone

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support Implementation of HB 812/SB 786

1 message

Sun, Feb 11, 2024 at 11:46 AM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission,

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations.

I applaud Maryland for being the first state to enact special protections for abortion health records. As an abortion provider and licensed family physician in Maryland and DC, I hear firsthand patients' fear and concern that someone will find out that they had an abortion in another state. Patients deserve to have their reproductive health decisions be kept confidential, private and safe. It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately.

Thank you,

Family Medicine

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Maryland’s privacy law regarding abortion records

1 message

Sun, Feb 11, 2024 at 9:21 AM

To: mhcc_regs.comment@maryland.gov

As a physician in state, I am writing to support Maryland’s legislation that would ensure the privacy of medical records related to abortion care. It is important that patients feel confident in the privacy and confidentiality of their medical care. In these days, unfortunately the political climate in some states puts people at risk of discrimination or even prosecution for having an abortion. The law in Maryland is an important model, and I will advocate for state to follow suit.
Sincerely,

Sent from the all new AOL app for iOS

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Physician letter of support for HB 812/SB 786 and proposed regulations

1 message

Sun, Feb 11, 2024 at 11:12 AM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

To Anna Gribble, Program Manager, Maryland Health Care Commission,

As a primary care physician, I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

I find it so inspiring that Maryland has the first law in the country with special privacy protections for abortion health records. Most people think their health records are protected under HIPAA; and that is true, but only to a certain extent. HIPAA allows their health records to be shared with any health care provider involved in their care. In fact, federal rules about electronic health records nearly require their complete health record be shared with their other providers.

What do these federal rules mean for patients? In most instances, these rules are positive for patients. It makes it easier for healthcare providers to coordinate your care. But after the Dobbs decision, these rules now put abortion patients, their support networks, and their providers at risk.

Thousands of people live in states that ban abortion. To seek abortion care, they are forced to travel to a safe state like Maryland. However, they are only truly safe if their abortion health records remain within the safe state. Unfortunately, electronic health record systems won't let this happen. These systems are designed to share a person's out-of-state health records with their home state providers. In states that ban abortion, this makes it easier for prosecutors, law enforcement, or even private citizens to obtain abortion records. They don't have to go out-of-state. Instead, they can use a subpoena or other legal instrument to try to obtain the information from a patient's home state provider.

With Maryland being the first state to enact special protections for abortion health records, health information systems, called health information exchanges and electronic health networks, are required to redesign their systems. If a patient has an abortion in Maryland, their health record must stay in Maryland, unless the patient expressly consents for the record to be share with another provider. **This is an essential step to ensuring that ensuring patients that get abortions in Maryland, their medical teams, and their support systems, are protected from prosecution.**

Please advocate that data segmentation and privacy protections be put in place by our medical record systems immediately. This is truly a time-sensitive issue.

Sincerely,

Sent via the Samsung Galaxy S22 Ultra 5G, an AT&T 5G smartphone
Get Outlook for Android

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

(no subject)

1 message

Sun, Feb 11, 2024 at 9:22 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations.

It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a volunteer for the Miscarriage and Abortion Hotline, I regularly hear patients' concerns that someone will flnd out that they have had an abortion in another state. I want to reassure them that this will not happen but I cannot. I know that currently medical records (including some abortion records) flow like water across state lines. I also know, that according to If/When/How, the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly. This legislation could begin to address these concerns.

I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients in the setting of an abortion, it means that those patients miss out on the other features of an EMR, such as the ability of providers to see records from specialty, radiology, or hospital visits.

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can’t wait!

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support for implementation of HB 812/SB 786

1 message

Mon, Feb 12, 2024 at 12:08 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission,

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

Thousands of people live in states that ban abortion. To seek abortion care, they are forced to travel to a safe state such as Maryland. Sadly, they are only truly safe if their abortion health records remain within the safe state. Unfortunately, current systems for electronic health record are not set up to protect those seeking abortions and prosecutors, law enforcement and even private citizens living in states that ban abortions can easily obtain their records.

As a primary care doctor, I applaud Maryland as the first state to enact special protections for abortion health records. It is urgent that data segmentation and privacy protections are put in place by our medical record systems. Thank you for leading the way!

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Abortion records

1 message

Sun, Feb 11, 2024 at 6:56 PM
To: mhcc_regs.comment@maryland.gov

Hi -
I am a family physician writing in support of Maryland's proposed legislation separating reproductive health records from the rest of a patient's medical records. With increased criminalization of abortion in many states, many patients are justifiably scared of having their medical records shared with out-of-state providers. Please help protect patients and their providers by passing this important legislation.
Sincerely

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

keep reproductive health records separate

1 message

Sun, Feb 11, 2024 at 5:57 AM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

As a reproductive health provider and primary care physician for over 20 years, I urge you to keep reproductive health records separate. This information , if shared across state lines, puts women at risk of harrassment , loss of privacy , and even criminal prosecution for reproductive health choices that are entirely legal. There is every reason to protect these health records and no practical, moral or medical reason to make it accessible across state lines.

Thank you for your consideration of this important issue.

Sent with Proton Mail secure email.

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support for careful separation within medical records

1 message

Sun, Feb 11, 2024 at 4:35 AM

To: mhcc_regs.comment@maryland.gov

Dear Maryland Commission of Health,

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland lead in the implementation of comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a volunteer for the miscarriage and abortion hotline, I regularly hear patients' concerns that someone will find out that they have had an abortion in another state. I want to reassure them that wont happen but I can't because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients' in the setting of abortion, it means that those patients miss out on the ability of providers to see records from specialty, radiology, or hospital visits,

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can't wait!

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

I support the implementation of HB 812/SB 786 with the proposed regulations

1 message

Mon, Feb 12, 2024 at 9:57 AM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

As a physician in , I am grateful for protection of health records regarding abortions, since know how important this is for my patients who are traveling from out of state, where out-of-state abortion is the only possible way for a woman to get the health care that she may need.

It is gratifying to know that Maryland offers similar protections and I hope that the law can be implemented as written.

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support for HB 812 / SB 786

1 message

Mon, Feb 12, 2024 at 4:43 PM

To: mhcc_regs.comment@maryland.gov

Dear Ms Gribble,

I'm writing in strong support of the implementation of HB812/SB786 with the proposed regulations. As a family medicine physician in who also provides abortion care for my patients, I've seen firsthand how necessary privacy regulations are to patient safety. I've had patients come to me from Texas for abortion care, then return to Texas to find that their electronic medical records had been automatically shared across state borders, without the patient consenting to this specifically. This has caused significant stress to my patients and their families, and is still ongoing as they fear what may happen with this information. I have to inform every single patient I see for an abortion, even those who live in that their electronic medical records may be shared with others across state lines. (Even though a similar bill passed in California, the EMRs and HIEs do not have the capability to segregate this data yet.) **In many cases I have resorted to using paper records**, as some patients have requested complete privacy and paper records are the best means I have to achieve that.

I applaud Maryland's efforts and hope this will be a model for other states all across the country. Thank you for all you are doing to protect patients during this time when certain forms of health care can be criminalized. I wish I could share with you directly the voices of patients who are so very grateful for this work.

Respectfully,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

New Privacy Law for Reproductive Infromation

1 message

Tue, Feb 6, 2024 at 7:29 AM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

I am writing in support of Maryland's proposed privacy law aimed to protect information about reproductive choices. I am an MFM physician and care for women who have devastating pregnancy complications and some choose to end the pregnancy. These are difficult decisions. I also work in healthcare IT and have supervised multiple HIE implemetnations. Our organization has had to put in place multiple safe gaurds to protect information – all of which rely on human intervention that is complicated and thus prone to failure. We need better tools to protect women's rights.

CONFIDENTIALITY NOTICE: This email transmission and any documents, files, or previous email messages attached to it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any further review, disclosure, copying, dissemination, distribution, or use of any of the information contained in or attached to this email transmission is strictly prohibited. If you have received this message in error, please notify the sender immediately by email, discard any paper copies, and delete all electronic files of the message. If you are unable to contact the sender or you are not sure as to whether you are the intended recipient, please call .

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

HB 812/SB 786

1 message

Sun, Feb 11, 2024 at 1:24 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a primary care provider, I often hear patients' concerns about the privacy of their sensitive records, including reproductive healthcare records. I want to reassure them that won't happen but I can't because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

I also am aware of multiple clinics that either use paper records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients' in the setting of abortion, it means that those patients miss out on the ability of providers to see records from specialty, radiology, or hospital visits,

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can't wait!

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Support for Maryland's Privacy Law for Abortion Records

1 message

Mon, Feb 5, 2024 at 9:46 PM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

I want to take a moment to commend Maryland on taking the lead in bolstering privacy protections for reproductive healthcare. These are very challenging times, and the right path forward is not perfectly clear, but Maryland's initiative has already created meaningful advances. Maryland's leadership has stimulated development by our EHR vendor partners to better protect privacy, even though prior advocacy by healthcare leaders had no effect on EHR technical approaches. Maryland is also paving the way for other states like mine, and it is reassuring to know that if my patients travel to Maryland that their privacy will be protected. I hope that the momentum for these needed changes will continue to pick up across other states around the country.

Thank you for your leadership,

I may send emails evenings and weekends as it works well for me, but I absolutely don't expect any responses back until regular work hours. If an issue is urgent, I will text or call.

CONFIDENTIALITY NOTICE: This communication and any attachments may contain confidential or privileged information for the use by the designated recipient(s) named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or the attachments is strictly prohibited. If you have received this communication in error, please contact me and destroy all copies of the communication and attachments. Thank you.

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

comments on privacy protections for abortion care

1 message

To: mhcc_regs.comment@maryland.gov Mon, Feb 12, 2024 at 10:11 AM

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As an abortion provider in Maryland, I regularly see patients from Maryland as well as all over the country. Patients who are afraid of getting care in their home state or worried about having medical records shared with providers that are not supportive of their decision. I want to reassure them about the safety of their medical records, but in today's IT and HIE environment, it is easy for records to move across systems, providers, and and state lines without a second thought. More importantly prosecutors, now have the abilitiy to criminalize abortion and miscarriage care so it has become more urgent to protect providers and patients.

We provide these protections for teens and for clients with behavioral health needs, so let's do the same for patients seeking abortion care.

Thank you for your support,

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Protect the privacy of medical records of reproductive health care

1 message

Sun, Feb 11, 2024 at 3:25 AM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a volunteer for the miscarriage and abortion hotline, I regularly hear patients' concerns that someone will flnd out that they have had an abortion in another state. I want to reassure them that wont happen but I can't because I know that currently medical records (including some abortion records) flow like water across state lines. I also know that according to If/When/How the most common way that pregnant people are criminalized is through a report to law enforcement from a healthcare worker. This worries me greatly.

I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients. While this helps to protect patients' in the setting of abortion, it means that those patients miss out on the ability of providers to see records from specialty, radiology, or hospital visits,

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can't wait!

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

support HB812/SB 786

1 message

To: mhcc_regs.comment@maryland.gov

Sun, Feb 11, 2024 at 7:40 PM

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As a family doctor I regularly hear patients' concerns that someone will find out that they have had an abortion in another state. I want to reassure them that won't happen but I can’t because I know that currently medical records (including some abortion records) flow like water across state lines. I also know of multiple clinics that either use paper medical records or are resisting upgrading to an EMR that has enhanced interoperability simply because they are afraid that their medical records of reproductive health care will be used against their patients.

It is essential that data segmentation and privacy protections be put in place by our medical record systems immediately. Patients and providers can’t wait!

Many thanks for all of your work and support,

Family Doctor

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Please support the implementation of HB 812/SB 786 with the proposed regulations

1 message

Mon, Feb 12, 2024 at 11:41 AM

To: "mhcc_regs.comment@maryland.gov" <mhcc_regs.comment@maryland.gov>

This message was transmitted over an encrypted connection.

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare. In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As an abortion provider in [redacted], I regularly see patients from [redacted] as well as all over the country. Some patients are (understandably) afraid of getting care in their home state or worried about having medical records shared with providers that are not supportive of their decision. I want to reassure them about the safety of their medical records, but in today's IT and HIE environment, it is easy for records to move across systems, providers, and state lines without a second thought. More importantly prosecutors, now have the ability to criminalize abortion and miscarriage care so it has become more urgent to protect providers and patients. We must put these extra protections in place.

We provide these protections for teens and for clients with behavioral health needs, so let's do the same for patients seeking abortion care.

Thank you for your support,

Sincerely,

MHCC_REGS COMMENT -MDH- <mhcc_regs.comment@maryland.gov>

Implementation of HB 812/SB 786

1 message

Mon, Feb 12, 2024 at 12:21 PM

To: mhcc_regs.comment@maryland.gov

Dear Anna Gribble, Program Manager, Maryland Health Care Commission

I am writing to support the implementation of HB 812/SB 786 with the proposed regulations. It is essential that Maryland implement comprehensive protections for medical records related to reproductive healthcare.

In this post-Dobbs world, we need to ensure the safety and security of people seeking abortion care, along with their providers and personal support networks.

As an abortion provider, I regularly see patients from all over the country. Patients who are afraid of getting care in their home state or worried about having medical records shared with providers that are not supportive of their decision. I want to reassure them about the safety of their medical records, but in today's IT and HIE environment, it is easy for records to move across systems, providers, and state lines without a second thought. More importantly prosecutors, now have the ability to criminalize abortion and miscarriage care so it has become more urgent to protect providers and patients.

We provide these protections for teens and for clients with behavioral health needs, so let's do the same for patients seeking abortion care.

Thank you for your support,

Sincerely,