

October 4, 2023

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

RE: Feedback on proposed amendments COMAR 10.25.07 and 10.25.18

Dear Executive Director Steffen and the Maryland Health Care Commission,

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

[COMAR 10.25.07, Certification of Electronic Health Networks and Medical Care Electronic Claims Clearinghouses](#)

[COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information](#)

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

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

AdvancedMD	eClinicalWorks	Flatiron Health	MEDITECH, Inc.	Oracle Cerner
Allscripts	Elekta	Foothold Technology	Modernizing Medicine	PointClickCare
Altera Digital Health	eMDs – CompuGroup Medical	Greenway Health	Netsmart	Sevocity
Athenahealth	EndoSoft	Harris Healthcare	Nextech	STI Computer Services
BestNotes	Epic	MatrixCare	NextGen Healthcare	TenEleven Group
CPSI	Experity	MEDHOST	Office Practicum	Varian – A Siemens Healthineers Company
CureMD				

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

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

We have provided detailed feedback in the attached table.

Thank you for your consideration,

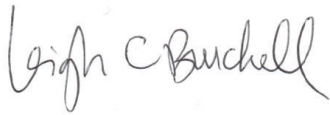


David J. Bucciferro
Chair, EHR Association
Foothold Technology

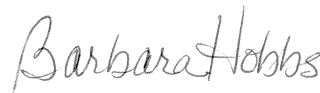


William J. Hayes, M.D., M.B.A.
Vice Chair, EHR Association
CPSI

HIMSS EHR Association Executive Committee



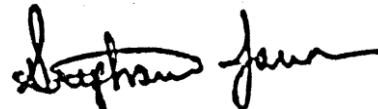
Leigh Burchell
Altera Digital Health



Barbara Hobbs
MEDITECH, Inc.



Cherie Holmes-Henry
NextGen Healthcare



Stephanie Jamison
Greenway Health



Ida Mantashi
Modernizing Medicine



Kayla Thomas
Oracle Cerner

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

		<p>under Health-General Article, §4-302.5, Annotated Code of Maryland, including:</p> <p>(a) Mifepristone data, as defined by the Secretary; and</p> <p>(b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to:</p> <p style="padding-left: 40px;">(i) Abortion care; and</p> <p style="padding-left: 40px;">(ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.</p>	<p>software solutions that will support Maryland providers, including:</p> <ol style="list-style-type: none"> 1. What code sets will be used? 2. Where will codes be published? 3. How often will codes be updated? 4. What are expectations for uncoded data, such as free text notes? <p>We suggest the following addition in bold and italics to clarify that legally protected health information is care delivered in Maryland:</p> <p>(40) “Legally protected health information” means the health information <i>about care delivered and received in Maryland after December 1, 2023</i> subject to restrictions under Health-General Article, §4-302.5, Annotated Code of Maryland, including:</p> <p>(a) Mifepristone data, as defined by the Secretary; and</p> <p>(b) As provided in COMAR XX.XX.XX, the diagnosis, procedure, medication, and other codes related to:</p> <p style="padding-left: 40px;">(i) Abortion care; and</p> <p style="padding-left: 40px;">(ii) Sensitive health services, as defined by Health-General, §4-301, Annotated Code of Maryland.</p>
4	Chapter 18.03 B(4)-(6)	<p>(4) An HIE shall make health care consumer educational materials readily available, at no charge, to participating organizations and [their users] the participating organizations’ users through distribution channels such as websites, postal mail, email, secure third-party smart phone applications, and any other reasonable media or distribution channel commonly used and generally available to the HIE and health care consumer.</p> <p>(5) In addition to the foregoing requirements, with regard to sensitive health information, the health care consumer educational content shall include: (a) The scope</p>	<p>We suggest that educational obligations be removed from developers of certified health IT, due to the definitional discrepancies identified in Row 1.</p> <p>Developers of certified health IT are unlikely to have direct relationships with patients or consumers. Patient education on health data exchange (and other similar topics) is conducted by healthcare providers who have a relationship with the patient and can contextualize what exchange consents might mean.</p> <p>Some healthcare organizations may vary in how they operationalize a patient’s right to opt in or out of use of</p>

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

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

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

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

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

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

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

[MHCC Commission Meeting Agenda, December 15, 2005 \(maryland.gov\)](#)

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

Chapter 07 Certification of Electronic Health Networks and Medical Care Electronic Claims

Clearinghouses

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

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

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