MARYLAND Health Care Commission

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

Final Regulations in Response to Chapter 249/House Bill 812, *Health – Reproductive Health Services – Protected Information and Insurance Requirements* (2023)

Prepared by the Maryland Division of State Documents

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*

mhcc.maryland.gov

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

4160 Patterson Avenue
Baltimore, MD 21215

MARYLAND Health Care Commission

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

Table of Contents

Title 10
MARYLAND DEPARTMENT OF HEALTH
Subtitle 25 MARYLAND HEALTH CARE COMMISSION
10.25.18 Health Information Exchanges: Privacy and Security of Protected Health Information

Authority: Health-General Article, §§4-301, 4-302.2, *4-302.3, 4-302.5,* 4-304, 19-101, and 19-143, Annotated Code of Maryland

.01 Scope and Purpose.

A. (text unchanged)

B. This chapter applies to:

(1) **[**A health information exchange**]** *An HIE,* as defined in Regulation **[**.02B(28)**]** *.02B(32)* of this chapter**[**;**]**, *including:*

(a) An individual or entity that determines, controls, or has discretion to administer any requirement, policy, or agreement that allows, enables, or requires the use of any technology or services for access, exchange, or use of electronic protected health information:

(i) Among more than two unaffiliated individuals or entities that are enabled 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 CFR §164.501, regardless of whether the individuals or entities are subject to the requirements of 45 CFR Parts 160 and 164; and

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

(2) A person who accesses, uses, or discloses protected health information through **[**a health information exchange**]** *an HIE*; and

(3) **[**A person who uses or discloses information derived or obtained from, or based on protected**]** *Electronic* health information **[**obtained or released through**]** *stored in,* or maintained by, an HIE.

C. This chapter does not apply to:

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

(a) (text unchanged)

(b) Among credentialed professionals of a hospital's medical staff; **[**or**]**

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

(d) Among entities under common ownership as defined at Health-General Article, §4-301, Annotated Code of Maryland, for health care treatment, payment, or health care operations purposes, as those terms are defined in 45 CFR §164.501;

(e) By a carrier, as defined in Insurance Article, §15-301, Annotated Code of Maryland, exchanging information as required by 45 CFR §156.221; or

(f) Between a carrier and its business associate, as defined in 45 CFR §160.103, if the organizational and technical processes provided or governed by the business associate are transactions, as defined in 45 CFR §160.103; or

(2) (text unchanged)

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.

[D.**]** *E.* The requirements in this chapter are in addition to those **[**required by**]** *set forth below*:

(1) The Health Insurance Portability and Accountability Act of 1996, **[**including all pertinent regulations (45 CFR §§160 and 164) issued by the U.S. Department of Health and Human Services, as amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5)**]** *and the pertinent regulations at 45 CFR Parts 160 and 164*;

(2) The Maryland Consumer Protection Act, **[**Maryland**]** Commercial Law Article, **[**§13-101 et seq.,**]** *Title 13,* Annotated Code of Maryland;

(3) The Maryland Personal Information Protection Act, Commercial Law Article, **[**§14-3501 et seq.,**]** *Title 14, Subtitle 35,* Annotated Code of Maryland;

(4) The Maryland Confidentiality of Medical Records Act, Health-General Article, Title 4, Subtitle 3, **[**Annotated Code of Maryland, including provisions regarding confidentiality of mental health records in Health-General Article §4-307,**]** Annotated Code of Maryland;

(5) Health General Article, §4-307, Annotated Code of Maryland, Confidentiality of Mental Health Records;

[(5)**]** *(6) 16 CFR Part 318,* Health Breach Notification Rule, **[**16 CFR §318,**]** adopted by the Federal Trade Commission pursuant to the HITECH Act;

[(6)**]** *(7)* 42 CFR Part 2 **[**regulations; and**]**, *Confidentiality of Substance Use Disorder Patient Records;*

(8) Titles IV and XI of the 21st Century Cures Act and the pertinent regulations, 45 CFR Part 171, and as defined at Regulation .02B(71) of this chapter; and

[(7)**]** *(9)* (text unchanged)

.02 Definitions.

A. (text unchanged)

B. Terms Defined.

(1) "*Adjudication of claims" means the activities necessary for the adjudication or subrogation of a health benefit claim that has been filed or may be filed by a patient, or with the authorization of a patient on the patient's behalf, including:*

(a) Determinations of eligibility or coverage, including coordination of benefits or the determination of cost-sharing amounts;

(b) Reasonable prospective, concurrent, or retrospective utilization review or predetermination of benefit coverage;

(c) Review, audit, and investigation of a specific claim for payment of benefits with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(d) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing; and

(e) Risk adjustments based on enrollee health status and demographic characteristics.

[(1)**]** *(2)* (text unchanged)

[(2)**]** *(3)* "Appropriate notice to one or more health care consumers" means notice, related to a request for *individually* identifiable **[**data**]** *health information* for secondary use, that meets the following requirements:

(a)—(b) (text unchanged)

[(3)**]** *(4)*—**[**(10)**]** *(11)* (text unchanged)

(12) "Commission" means the Maryland Health Care Commission.

[(11)**]** *(13)*—**[**(16)**]** *(18)* (text unchanged)

[(17)**]** *(19)* "Disclose" or "disclosure" means the release, redisclosure, transfer, provision, access, transmission, communication, or divulgence in any other manner of *health* information **[**in a medical record**]**, including an acknowledgment that a **[**medical**]** *health* record on a particular patient or recipient exists, outside the entity holding **[**such**]** *the* information.

[(18)**]** *(20)* (text unchanged)

(21) "Electronic health information" means health information that is in an electronic form.

[(19)**]** *(22)*—**[**(21)**]** *(24)* (text unchanged)

[(22)**]** *(25)* "External and independent review committee" means a group of individuals that:

(a) Is responsible for reviewing and making a determination regarding a request for a waiver of authorization related to population **[**care**]** *health* management; and

(b) (text unchanged)

[(23)**]** *(26)*—**[**(24)**]** *(27)* (text unchanged)

(28) "Health care" has the meaning provided in Health-General Article, §4-301(g), Annotated Code of Maryland.

[(25)**]** *(29)* "Health care consumer" *or "consumer"* means *a recipient,* a patient, or a person in interest, as defined in this regulation.

[(26)**]** *(30)* (text unchanged)

[(27)**]** *(31)* "Health information" means any information, whether oral or recorded in any form or medium, *including electronic health information,* that:

(a)—(b) (text unchanged)

[(28)**]** *(32)* "Health information exchange" or "HIE" **[**means an entity that creates or maintains an infrastructure that provides organizational and technical capabilities in an interoperable system for the electronic exchange of protected health information among participating organizations not under common ownership, in a manner that ensures the secure exchange of protected health information to provide care to patients. An HIE includes a payor HIE but does not include an entity that is acting solely as a health care clearinghouse, as defined in 45 CFR §160.103. A payor may act as, operate, or own an HIE subject to these regulations.**]** *has the meaning provided in Health-General Article §4-301(i), Annotated Code of Maryland.*

(33) "Health information technology developer of certified health information technology" or "developer" means an entity that develops, sells, licenses, provides, or offers health information technology, as defined in 42 U.S.C. 300jj(5), to persons in the State and has one or more health information technology modules certified under a program that is kept or recognized by the National Coordinator in accordance with 42 U.S.C. 300jj-11(c)(5).

(34) Health Record.

(a) "Health record" means any health information, in any form or medium, created or transmitted by a participating organization or health care consumer that:

(i) Is entered in the record of a patient or recipient; and

(ii) Identifies or can readily be associated with the identity of a patient or a recipient.

(b) "Health record" includes a medical record as defined in Health-General §4-301(k), Annotated Code of Maryland.

[(29)**]** *(35)*—**[**(31)**]** *(37)* (text unchanged)

[(32)**]** *(38)* "Hospital" **[**means an institution defined**]** *has the meaning provided* in Health-General Article, §19-301(f), Annotated Code of Maryland**[**, that is licensed by the Office of Health Care Quality**]**.

[(33) "Identifiable data" means any health information that includes personal identifiers, as detailed in 45 CFR §164.501.**]**

(39) "Individually identifiable health information" has the meaning provided in 45 CFR §160.103 and includes any health information that contains personal identifiers, as detailed in 45 CFR §164.514(b).

[(34)**]** *(40)* (text unchanged)

(41) "Interoperability" has the meaning provided in 45 CFR §170.102.

(42) "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; and

(b) As specified by the Secretary, 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.

[(35)**]** *(43)*—**[**(46)**]** *(54)* (text unchanged)

[(47)**]** *(55)* "Person in interest" means any of the following, but does not include a participating organization:

(a)—(d) (text unchanged)

(e) If **[**§B(45)(d)**]** *§B(55)(d)* of this regulation does not apply to a minor:

(i)—(ii) (text unchanged)

(f) (text unchanged)

[(48)**]** *(56)* (text unchanged)

[(49)**]** *(57)* "Population **[**care**]** *health* management purpose" means the use of data, for secondary use, available from or through an HIE for population-based activities relating to the improvement of patient and population health or the reduction of health care costs, including but not limited to:

(a)—(d) (text unchanged)

[(50)**]** *(58)*—**[**(57)**]** *(65)* (text unchanged)

[(58)**]** *(66)* "Sensitive health information" means a subset of PHI, which consists of:

(a) Part 2 information; **[**or**]**

(b) Legally protected health information; or

[(b)**]** *(c)* Any other information that has specific legal protections in addition to those required under HIPAA or the Maryland Confidentiality of Medical Records Act**[**,which include, but are not limited to, Health-General Article, §4-307, Annotated Code of Maryland, and the Public Health Services Act, 42 U.S.C. §290dd-2, as implemented and amended in federal regulations**]**.

[(59)**]** *(67)*—**[**(62)**]** *(70)* (text unchanged)

(71) "21st Century Cures Act" means the 21st Century Cures Act, P.L. 114-255, as amended, and the pertinent regulations at 45 CFR Parts 156, 170, and 171 and 42 CFR Parts 422, 431, 438, 457, 482, and 485.

[(63)**]** *(72)*—**[**(65)**]** *(74)* (text unchanged)

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

A. (text unchanged)

B. An HIE shall provide needed information about the HIE to a health care consumer whose protected health information is maintained by a health information exchange, or may be accessed, used, or disclosed through the HIE.

(1)—(3) (text unchanged)

(4) An HIE shall make health care consumer educational materials readily available, *at no charge,* to participating organizations and **[**their users**]** *the participating organizations' users through distribution channels such as websites, postal mail, email, secure third-party smart phone applications, and any other reasonable media or distribution channel commonly used and generally available to the HIE and health care consumer.*

(5) In addition to the foregoing requirements, with regard to sensitive health information, the health care consumer educational content shall include:

(a) The scope of sensitive health information;

(b) The health care consumer's right to control sensitive health information;

(c) The method by which to engage in the granular patient consent process;

(d) The method or methods by which the health care consumer can access the patient's own sensitive health information;

(e) The circumstances under which an HIE must restrict or may disclose legally protected health information; and

(f) The method by which a health care consumer can request that a patient's legally protected health information be disclosed to a specific health care provider.

(6) When an HIE updates its health care consumer educational content, the HIE shall timely make the updated materials available to health care consumers.

C.—F. (text unchanged)

G. The following requirements shall apply to all communications between an HIE and a health care consumer**[**.**]***:*

(1) (text unchanged)

(2) A health care consumer's communication opting out or opting in to an HIE shall be made **[**in**]**:

(a) **[**Writing**]** *In writing*;

(b) (text unchanged)

(c) By telephone, if the HIE confirms the action with a written communication to the health care consumer in accordance with **[**§F(5)(a)—(b)**]** *§G(5)(a) and (b)* of this regulation.

(3)—(6) (text unchanged)

H. (text unchanged)

.04 Access, Use, or Disclosure of Sensitive Health Information.

A. Consistency with Disclosure Requirements Under Federal and State Law.

(1) A person shall comply with all relevant State and federal laws, including 42 CFR Part 2, *and Health-General Article, §4-302.5, Annotated Code of Maryland,* concerning the access, use, or disclosure of sensitive health information through an HIE and maintenance of such information by an HIE.

(2) (text unchanged)

(3) **[**Notwithstanding §A(2) of this regulation, an HIE may transmit sensitive health information:

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

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

(4)—(5) (text unchanged)

B. (text unchanged)

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; 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.

.06 Auditing Requirements.

A. In order to ensure that only an authorized user who is appropriately authenticated is granted access to HIE information, an HIE shall:

(1) Develop and implement protocols, methodologies, and a monitoring approach designed to discover any unusual finding, which may be identified within an audit of the user access logs, including conducting ongoing electronic monitoring of user access logs and investigate any unusual findings in accordance with this chapter**[**.**]***;*

(2) (text unchanged)

(3) **[**At least monthly, conduct**]** *Conduct* random audits of the user access logs to identify any unusual finding; and, if the HIE has been notified about an unusual finding or has reason to believe that inappropriate access has occurred, **[**more frequently than monthly.**]** *conduct random audits at least every other week until the unusual finding or inappropriate access has been mitigated;*

(4) At least quarterly, conduct 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;

[(4)**]** *(5)* (text unchanged)

[(5)**]** *(6)* Resolve **[**the matter surrounding**]** an unusual finding by:

(a) (text unchanged)

(b) Taking remedial action under Regulation .07 of this chapter**[**.**]***;*

[(6)**]** *(7)* Report any unusual finding to each participating organization involved in the unusual finding, as follows:

(a) If the unusual finding involves fewer than 10 patients, **[**in a timely manner**]** *within 5 business days after the unusual finding is discovered*;

(b) If the unusual finding involves between 10 and 50 patients, within 2 business days *after the unusual finding is discovered*; and

(c) If the unusual finding involves more than 50 patients, within 1 business day *after the unusual finding is discovered*; and

[(7)**]** *(8)* Maintain an audit trail of user access logs in a retrievable storage medium**[.]**, *as follows:*

(a) (text unchanged)

(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.

[(b)**]** *(c)* (text unchanged)

B. When an HIE has identified a potential *breach or non-HIPAA* violation **[**of this chapter**]**, the HIE shall conduct an unscheduled audit *within 30 days* that **[**shall**]**:

(1) **[**Gather**]** *Gathers* relevant information to determine if there is a violation;

(2) **[**Reflect] *Reflects* the size and scope of the potential violation; and

(3) [Comply**]** *Complies* with Regulation .08 of this chapter.

C. An HIE shall **[**conduct an annual privacy and security audit in**]** *at least annually enlist a qualified independent auditing firm to audit its privacy, security, and legal* compliance *in accordance* with the following provisions**[.]***:*

(1) The audit shall **[**be aimed at detecting patterns of inappropriate access, use, maintenance, and disclosure of information that are in violation of this chapter;**]***:*

(a) Assess potential risks to protect the confidentiality, integrity, and security of PHI;

(b) Assess operational compliance with State and federal law, including the requirements of this chapter;

(c) Be designed to determine the adequacy of business and technology-related controls, policies, and procedures and other safeguards employed by third-party service organizations based on industry standards and best practices; and

(d) Include an assessment of cybersecurity posture and compliance with this chapter, applicable provisions in HIPAA and HITECH, and recognized security practices by way of accreditation or certification from a nationally recognized entity.

(2) An HIE shall develop auditing policies and procedures for the independent auditor to conduct such an audit, which shall include, at a minimum:

(a) The scope of the audit;

(b) A description of all third-party organizations and processes to review and assess related privacy and security controls and audit reports;

(c) Interviews with relevant staff, including those from third-party service organizations, as appropriate;

(d) Names and contact information of all persons responsible for reviewing and maintaining privacy and security to include the implementation of corrective actions to address apparent gaps; and

(e) Time frames for completing audits and related activities.

[(2)**]** *(3)* An HIE shall provide the audit findings to the Commission in **[**compliance**]** *accordance* with Regulation .09 of this chapter**[**; and**]**.

[(3) At the request of the Commission, an HIE shall utilize a qualified third party to conduct an audit on the access, use, and disclosure of information through and the maintenance of information by the HIE.**]**

(4) If an audit detects unusual findings, an HIE shall investigate and resolve the matter in accordance with this regulation.

D. Upon the request of the Commission and consistent with the specifications in such request, an HIE shall:

(1) Provide *a summary of* the results of any audit that is required by this chapter, and any **[**supporting documentation**]** *corrective action plans identified by the audit, to the Commission*; and

(2) Conduct an additional unscheduled audit *within 180 days of the request* and provide the results of such an audit to the Commission within the time frame specified by the Commission.

E. If an HIE's audit reveals information that demonstrates a pattern of inappropriate access, use, maintenance, or disclosure of information that constitutes a breach or *non-HIPAA* violation **[**of this chapter**]**, or if the health information of more than ten patients was improperly used, accessed, maintained, or disclosed during the 12 months prior to the audit, then:

(1) The HIE shall use the findings from the audit to:

(a) Educate and train **[**a**]** *all impacted persons, which may include its workforce,* participating **[**organization or an**]** *organizations, and* authorized **[**user**]** *users* on proper access, use, and disclosure of information through or from the HIE**[**, as appropriate; or**]***; and*

(b) Evaluate and implement new control measures, including policies, procedures, or technology, to ensure proper use and access of the HIE**[**, as appropriate.**]***; and*

(2) (text unchanged)

[(3) The HIE shall post a publicly available summary report of the audit on the home page of its website within 30 days after completion of the audit and the Commission shall also post the report on the home page of its website.**]**

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; and

(2) The HIE shall take the appropriate measures specified in the Regulation. 07 of this chapter.

[F.**]** *G.* (text unchanged)

.07 Remedial Actions to Be Taken by an HIE.

A.—B. (text unchanged)

C. If an HIE has a reasonable belief that a *breach or* non-HIPAA violation **[**or breach under HIPAA**]** has occurred, either as a result of an investigation or otherwise, the HIE **[**shall carry out the following actions. Unless another time period is set forth below, the HIE shall act within 10 business days after acquiring the reasonable belief.**]** *shall:*

[(1) The HIE shall determine any remedial action necessary to address the breach or violation;

(a) The HIE may require that a remedial action include steps to correct an underlying problem.

(b) The HIE shall provide an appropriate and reasonable time frame for implementing the remedial action.

(2) The HIE shall provide the following to the Commission, to the participating organization, and to each person whom the investigation indicates may have committed a breach or violation:**]**

(1) For a breach, follow Regulation .08 of this chapter and federal breach notification requirements and timelines;

(2) For non-HIPAA violations, submit a corrective action plan to the Commission within 10 business days of conclusion of its investigation, which shall include:

(a) Any remedial action necessary to address the breach or violation as soon as practicable;

(b) Any steps necessary to correct the underlying problem, such as a change in processes or procedures, new technology, and training; and

(c) An appropriate and reasonable time frame for implementing the remedial action;

(3) Within a reasonable time frame, but in no event more than 10 business days following the investigation, provide the following to the Commission, and to the participating organizations:

(a) A copy of the findings of the investigation, excluding any *PHI or* sensitive health information;

(b)—(c) (text unchanged)

(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**[.]***;*

[(3)**]** *(4)* **[**The HIE shall immediately**]** *Immediately* suspend access **[**for an authorized user or participating organization**]** *of a person* when one of the following occurs:

(a) Available information demonstrates a significant breach by **[**a**]** *the* person;

(b) Available information demonstrates a significant non-HIPAA violation by [a] *the* person;

(c) Available information demonstrates a violation of State or federal law relevant to privacy or security by **[**a**]** *the* person;

(d) **[**A**]** *The* person has sold health information accessed through the HIE in violation of these regulations;

(e) **[**A**]** *The* person has failed to carry out the remedial actions identified by the HIE; or

(f) The Commission issues a request for suspension of **[**a**]** *the* person as provided in Regulation .09 of this chapter**[.]***; and*

[(4)**]** *(5)* **[**The HIE shall notify**]** *Notify* the health care consumer pursuant to Regulation .08 of this chapter, if such notification is required under applicable law, including HIPAA, or if so directed by the Commission **[**due to the seriousness of the non-HIPAA violation**]**.

D.—F. (text unchanged)

.09 Registration and Enforcement.

A. To operate an HIE in the State, a person shall be recognized by the Commission as having met requirements for registration.

(1) (text unchanged)

(2) Financial Integrity.

(a) Following review of the financial statement provided by the HIE under **[**Regulation .09A(1) of this chapter,**]** *§A(1)(b) of this regulation,* the Commission may require a bond, letter of guarantee, or other financial instrument from the HIE, its parent company, or other responsible person.

(b)—(e) (text unchanged)

(3) (text unchanged)

B. (text unchanged)

C. The Commission may take an enforcement action against a person **[**where**]** *when* there is reasonable basis to believe that the person has violated a provision of this chapter.

(1) The Commission may conduct any investigation into a potential violation.

(a) (text unchanged)

(b) A person shall provide information sought by Commission staff within 10 business days of its request for such information, unless an extension of time is sought for good cause shown and granted *by the Commission*.

(2) After **[**needed**]** *an* investigation *under §C(1) of this regulation,* the Commission staff may issue a notice of proposed action that includes **[**the following**]**:

(a) The details regarding each *violation or* potential violation;

(b) **[**The corrective action plan, if any, that the Commission staff recommends, which may include any of the following:**]** *A request for a person to submit a corrective action plan in order to achieve compliance with this chapter, which may include:*

(i)—(ii) (text unchanged)

(c) A recommended resolution of the potential violation, which may include:

(i)—(iii) (text unchanged)

(iv) Suspension of *HIE* registration or a person's access to information through an HIE; **[**or**]**

(v) Revocation of *HIE* registration or a person's access to information through an HIE**[.]***;*

(vi) Financial penalties in accordance with §C(3) of this regulation; or

(vii) Referral to another State or federal agency for civil or criminal enforcement.

(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 imposed by the Commission not exceeding $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.

(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.

[(3)**]** *(4)* (text unchanged)

D.—E. (text unchanged)

F. The Commission may coordinate with the Office of Attorney General**[**, Consumer Protection Division**]** concerning any potential violation involving a matter within the Attorney General's authority pursuant to State or federal law.

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 Commission, attesting that the HIE has been in full compliance with the requirements of this chapter for the 12-month period prior to the audit.

[G.**]** *H.* (text unchanged)

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

A. An HIE may not use or disclose a patient's sensitive health information for secondary use unless permitted by applicable federal or State laws and regulations.

[A.**]** *B.* Population **[**Care**]** *Health* Management.

(1) An HIE may disclose de-identified data or a limited data set, *as defined at 45 CFR §164.514(e),* to a care management organization for purposes related to population **[**care**]** *health* management, if approval is obtained from an internal review committee designated by the care management organization, which has:

(a) (text unchanged)

(b) Attested that the request is:

(i) For population **[**care**]** *health* management purposes; and

(ii) (text unchanged)

(2) An HIE may disclose *individually* identifiable **[**data**]** *health information* to a care management organization for purposes related to population [care] *health* management, if:

(a) The requirements of **[**§A(1)(a) and (b)**]** *§B(1)* of this regulation are met;

(b) Appropriate notice has been provided to health care consumers whose information is being requested, and either:

(i) (text unchanged)

(ii) An external and independent review committee has waived the need for the requesting entity to obtain authorization from those health care consumers who were provided appropriate notice, in accordance with Regulation **[**.02B(2)**]** *.02B(3)* of this chapter; and

(c) (text unchanged)

(3) (text unchanged)

(4) An HIE may not disclose a patient's sensitive health information for population **[**care**]** *health* management purposes unless permitted by applicable federal and State laws and regulations.

[B.**]** *C.* Research.

(1) An HIE may disclose de-identified data to a qualified research organization for research purposes if a privacy board has evaluated and confirmed that the:

(a) (text unchanged)

(b) Requested data to be disclosed:

(i)—(iii) (text unchanged)

(iv) Meets the de-identification standard and specifications in accordance with **[**45 CFR**]** 45 CFR §164.514(a)—(c).

(2) An HIE may disclose *individually* identifiable **[**data**]** *health information* to a qualified research organization for research purposes if:

(a) (text unchanged)

(b) The IRB or privacy board has evaluated the request and confirmed that the requirements of **[**§B(1)(a) and (b)(i)—(iii)**]** *§C(1)(a) and (b)(i)—(iii)* of this regulation are met.

(3) If an IRB or privacy board does not waive or alter the requirement of authorization from health care consumers whose *individually* identifiable **[**data**]** *health information* is to be disclosed, an HIE may only disclose *individually* identifiable **[**data**]** *health information* of health care consumers who have provided authorization, which must meet the requirements as set forth in 45 CFR §164.508.

(4) If an IRB or privacy board declines jurisdiction, then the disclosure of *individually* identifiable **[**data**]** *health information* may only be made if health care consumer authorization is obtained.

(5) As part of an HIE's data use agreement with an entity to which it disclosed *individually* identifiable **[**data**]** *health information* for secondary use, there **[**must**]** *shall* be oversight by an IRB or privacy board for the duration of the research use.

(6)—(8) (text unchanged)

(9) An HIE may not disclose a patient's sensitive health information for research **[**purpose**]** *purposes* unless permitted by applicable federal or State laws and regulations.

[C.**]** *D.* Enforcement and Reporting.

(1)—(2) (text unchanged)

(3) An HIE shall report at least annually to the Commission and more frequently, if requested by the Commission, regarding the release of information for population **[**care**]** *health* management. The Commission may:

(a) Require a care management organization to provide additional information for review by the Commission or the Commission's designated third party regarding the care management organization's use of data from an HIE for population **[**care**]** *health* management;

(b)—(d) (text unchanged)

(4) (text unchanged)

.11 Requirements for Accessing, Using, or Disclosing of Data Through an HIE in an Emergency.

A. (text unchanged)

B. If an HIE's emergency access policy allows the disclosure of information during an emergency, the HIE shall:

(1)—(4) (text unchanged)

(5) Maintain an audit trail of user emergency access logs in accordance with **[**.06A(6)(d)**]** Regulation *.06A(8)* of this chapter; and

(6) (text unchanged)

MARYLAND Health Care Commission

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

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

Table of Contents

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

Authority: Health-General Article, §§4-302.1, *4-302.5*, 19-103(c)(2), (9), and (10), 19-109(a)(1), 19-134, and 19-135(a) and (b), Annotated Code of Maryland

.02 Definitions.

A. (text unchanged)

B. Terms Defined.

(1) "*Adjudication of claims" means the activities necessary for the adjudication or subrogation of a health benefit claim that has been filed or may be filed by a patient, or with the authorization of a patient on the patient's behalf, including:*

(a) Determinations of eligibility or coverage, including coordination of benefits or the determination of cost-sharing amounts;

(b) Reasonable prospective, concurrent, or retrospective utilization review or predetermination of benefit coverage;

(c) Review, audit, and investigation of a specific claim for payment of benefits with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(d) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing; and

(e) Risk adjustments based on enrollee health status and demographic characteristics.

[(1)**]** *(2)* (text unchanged)

(3) "Disclose" or "disclosure" means the release, redisclosure, transfer, provision, access, transmission, communication, or divulgence in any other manner of health information, including an acknowledgement that a health record on a particular patient or recipient exists outside the entity holding the information.

[(2)**]** *(4)*—**[**(5)**]** *(7)* (text unchanged)

(8) "Health information" means any information, whether oral or recorded in any form or medium, including electronic health information, that:

(a) Is created or received by a health care provider, health plan, public health authority, employe, life insurer, or health care clearinghouse; and

(b) Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

(9) "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; and

(b) As specified by the Secretary, 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.

[(6)**]** *(10)*—**[**(9)**]** *(13)* (text unchanged)

[(10)**]** *(14)* "Qualified accreditation or certification organization" means **[**the Electronic Healthcare Network Accreditation Commission (EHNAC) or an organization recognized by the Executive Director that has established standards of quality for electronic health networks and accredits or certifies networks that meet those standards**]** *a nationally recognized entity that has established privacy and security standards for electronic health networks and accredits or certifies networks that meet those standards.*

.04 Procedure to Obtain Certification.

A. (text unchanged)

B. Fees.

(1) An application fee shall be paid to the Commission **[**at the time the MHCC Electronic Health Network Certification application is filed**]** *within 30 days of receipt of an invoice from the Commission.*

(2) For an electronic health network with one operational site, an application fee of $400 shall be paid **[**at the time the application is filed**]** *within 30 days of receipt of an invoice from the Commission.*

(3) For an electronic health network with more than one operational site, an application fee of $400, plus a $200 fee for each additional operational site, shall be paid **[**at the time the application is filed**]** *within 30 days of receipt of an invoice from the Commission.*

.05 Standards for Certification.

A. In order to obtain certification, an applicant shall:

(1) (text unchanged)

(2) Meet the following standards for certification:

(a) Demonstrate compliance with the HIPAA privacy standards set forth in 45 [C.F.R. §§160 and 164] *CFR Parts 160 and 164*;

(b) Demonstrate compliance with HIPAA security standards set forth in 45 [C.F.R. §§160, 162, and 164] *CFR Parts 160, 162, and 164*;

(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 Code of Maryland;

[(c)**]** *(d)*—**[**(e)**]** *(f)* (text unchanged)

B. (text unchanged)

.09 Withdrawal of Certification *and Other Penalties*.

A. The Commission may withdraw certification from an MHCC-certified EHN if the Commission finds that:

[A.**]** *(1)* (text unchanged)

[B.**]** *(2)* A principal or owner of the MHCC-certified EHN, or the entity itself, is convicted of, or pleads guilty or nolo contendere to, a crime related to the operation of the EHN or to a crime involving financial improprieties; **[**or**]**

[C.**]** *(3)* A principal or owner of the MHCC-certified EHN, or the entity itself, is notified by a qualified accreditation or certification organization or the Commission of a violation of HIPAA privacy or security standards and fails to take action to remedy the violation within the period of time specified by a qualified accreditation or certification organization or by the Commission**[**.**]***;*

(4) The MHCC-certified EHN disclosed legally protected health information in violation of Health-General Article, §4-302.5, Annotated Code of Maryland; or

(5) The MHCC-certified EHN violated a provision of COMAR 10.25.18.

B. An MHCC-certified EHN shall report on compliance progress to the Commission, as follows:

(1) By January 8, 2024, an MHCC-certified EHN shall submit to the Commission:

(a) An affirmation that to the extent required by Health-General Article, §4-302.5, Annotated Code of Maryland, it:

(i) Possesses 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; 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 January 8, 2024, including a detailed explanation of the EHN's limitations;

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

(iii) A timeline to implement Health-General Article, §4-302.5, Annotated Code of Maryland, 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) of this regulation, 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.