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

Informal Draft Amendments

For Public Comment

May 15, 2024

The Maryland Health Care Commission (MHCC) seeks public comment on informal draft amendments to COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information.* The draft amendments generally support implementation of the following legislation passed by the Maryland General Assembly in 2021 and 2022:

- Chapter 790/791, *Public Health - State Designated Exchange - Clinical Information* (2021)
- Chapter 798, *Health Information Exchanges - Electronic Health Information - Sharing and Disclosure* (2021)
- Chapter 296, *Public Health - State Designated Exchange - Health Data Utility* (2022)

The MHCC kindly requests comments specific to provisions supporting the 2021 and 2022 laws at this time. The provisions are in green font and underlined on pages 2-58 that follow. Please note, there will be other opportunities to comment on the regulations.

When submitting written comments, please reference all applicable page numbers and regulation number(s), section(s), and subsection(s), adhering to the COMAR Codification System. Please submit comments as an attachment in an email to mhcc_regs.comment@maryland.gov by close of business on May 29, 2024. The MHCC cannot ensure that comments received after the due date will be considered. For questions, please contact Anna Gribble at anna.gribble1@maryland.gov.

Title 10 MARYLAND DEPARTMENT OF HEALTH

Subtitle 25 MARYLAND HEALTH CARE COMMISSION

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

Authority: Health-General Article, §§4-301, 4-302.2, 4-302.3, 4-302.5, 4-304, 19-1031, ~~and~~ 19-143, and 19-145, Annotated Code of Maryland

Table of Contents

.01 Scope and Purpose.

A. This chapter addresses the privacy and security of protected health information maintained by a health information exchange, or obtained or released by any person through a health information exchange by adopting specific requirements:

(1) To assure the privacy and security of protected health information accessed, used, or disclosed through a health information exchange, including protections for the secondary use of protected health information obtained, accessed, or released through a health information exchange;

(2) To govern the access, use, maintenance, and disclosure of protected health information through or by a health information exchange;

(3) To improve access to clinical records by treating clinicians; and

(4) To promote uses of a State-designated HIE that will assist public health agencies in reaching public health goals.

B. This chapter applies to:

(1) An HIE, as defined in Regulation .02B(3~~82~~) 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(3~~93~~) of this chapter;

(2) A person who accesses, uses, or discloses protected health information through an HIE; ~~and~~

(3) Electronic health information stored in, or maintained by, an HIE; and~~.~~

(4) A dispenser authorized by law to dispense noncontrolled prescription drugs to a patient or the patient's agent in the State.

C. This chapter does not apply to:

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

(a) Between a hospital and a credentialed professional;

(b) Among credentialed professionals of a hospital's medical staff;

(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) The use, access, or disclosure of protected health information using point-to-point transmission unless an HIE is involved in the transmission of the data.

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.

E. The requirements in this chapter are in addition to those set forth below:

(1) The Health Insurance Portability and Accountability Act of 1996, and the pertinent regulations at 45 CFR Parts 160 and 164;

(2) The Maryland Consumer Protection Act, Commercial Law Article, Title 13, Annotated Code of Maryland;

(3) The Maryland Personal Information Protection Act, Commercial Law Article, 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;

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

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

(7) 42 CFR Part 2, 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(7~~8~~1) of this chapter; and

(9) All other applicable State and federal laws and regulations governing the use, access, maintenance, and disclosure of health information.

F. Nothing in this chapter shall prohibit:

(1) The Maryland Department of Health, the Commission, or the Health Services Cost Review Commission from using electronic health information, subject to federal and State law, for health regulatory and public health functions;

(2) The sharing or disclosing of information that is required to be exchanged under Title 21, Subtitle 2A of the Health-General Article; or

(3) The sharing or disclosing of information that is required to be exchanged under federal law, including for the purposes of payment, as defined in 45 CFR § 164.501.

.02 Definitions.

A. In this chapter, the following terms have the meanings indicated.

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.

(2) "Ancillary clinical service provider" means a health care provider who has a direct contractual agreement with the hospital to provide therapeutic, diagnostic, or custodial ancillary services for the hospital as part of its affiliation. Ancillary services may include skilled nursing, home care, outpatient rehabilitation and therapy, transportation, ambulatory surgery, dialysis, laboratory, radiology, pharmacy, and chemotherapy.

~~(2)~~(3) "Application Programming Interface" or "API" means a set of functions and procedures allowing the creation of applications that meets the requirements of 45 CFR § 170.404 and 45 CFR § 170.315(g)(7) through (10).

~~(3)~~(4) "Appropriate notice to one or more health care consumers" means notice, related to a request for individually identifiable health information for secondary use, that meets the following requirements:

(a) The notice:

(i) Must include educational information pertaining to the requesting entity's secondary use of data obtained through an HIE, including why the entity is requesting the data and how it intends to use the data;

(ii) May describe an ongoing scenario such as care coordination or other ongoing care management activities against which subsequent data may be requested by the care management organization from the HIE; in such cases, the potential need for and nature of such requests shall be included in the description of the initial request to the external review board and shall be plainly documented in the notice to health care consumers;

(iii) Must include a clear and detailed description of the steps a health care consumer must take in order to grant authorization for the use of their information or to deny authorization;

(iv) Must provide clear, detailed notice that the health care consumer's failure to respond could result in their information being disclosed without their authorization, if an independent external review committee waives authorization; and

(v) Must have characteristics detailed in Regulation .03B(2)(b)—(g) of this chapter.

(b) The care management organization, or its third party, has provided to each health care consumer whose identifiable information is being requested:

(i) Notice as described above, using varied methods, where possible, to reach the health care consumer;

(ii) The opportunity to submit authorization or denial of authorization through various methods such as email, online, mail, and phone; and

(iii) At least 30 calendar days from the time of the first notice to respond to the notice.

~~(4)~~(5) "Authentication" means the process of establishing confidence in user identities electronically presented to an information system.

~~(5)~~(6) "Authorization" has the meaning provided in 45 CFR §164.508.

~~(6)~~(7) "Authorized purpose" means the specific reason consistent with this chapter and State and federal law for which an authorized user may use, access, or disclose protected health information through or from an HIE. The authorized purpose may include daily operations and maintenance of the HIE for:

(a) The staff of the HIE who has signed a confidentiality and nondisclosure agreement; and

(b) The staff of the HIE's contractor if the contractor:

(i) Has entered into a business associate agreement with the HIE; and

(ii) Has contractually agreed to limit access to the HIE only to its employees, agents, and independent contractors with a need-to-know; and who are under a confidentiality restriction, which may include a binding work force policy and procedure.

~~(7)~~(8) "Authorized user" means an individual identified by a participating organization or a health information exchange, including a health care consumer, who may use, access, or disclose protected health information through or from a health information exchange for a specific authorized purpose and whose HIE access is not currently suspended or terminated under Regulation .05, .07, or .09 of this chapter.

~~(8)~~(9) "Breach" has the meaning provided in 45 CFR §164.402.

(10) "Business associate" has the meaning provided in 45 CFR §160.103.

~~(9)~~(11) "Business day" means any day except Saturday, Sunday, or a holiday on which State offices are closed.

~~(10) "Core elements of the Master Patient Index (MPI)" are the minimum elements that are:~~

~~(a) Required for an HIE to identify a particular patient across separate clinical, financial, and administrative systems; and~~

~~(b) Needed to exchange health information electronically.~~

~~(11)~~(12) "Care management organization", in the context of secondary use, means any entity that:

(a) Has a financial or specific care-related responsibilities for individuals with whom they may not have a treatment, payment, or health care operations relationship under 45 CFR §164.501(1); and

(b) Has the legal or regulatory authority to exercise the responsibilities stated in §B(10)(a) of this regulation; or

(c) Is operating in accordance with Maryland's All-Payer Model or successor agreement between the Centers for Medicare and Medicaid Services and the State of Maryland;

(d) Does not include a third-party entity engaged by a participating organization to provide care management services on behalf of such participating organization for a primary use.

~~(12)~~(13) "Commission" means the Maryland Health Care Commission.

(14) "Consent management application" means a software tool or platform designed to request, receive, store, and manage a person in interest's consent preferences regarding the sharing of the patient's electronic health information through an HIE.

~~(13)~~(15) "Control" means providing a method by which the health care consumer can electronically provide instructions to an HIE regarding the disclosure of the patient's information being made available through the HIE, which may include specifying:

(a) The individuals and organizations to whom the HIE may disclose the patient's health information;

(b) The circumstances (e.g., all, emergency only, inpatient, etc.) under which the patient's health information may be disclosed through the HIE; and

(c) What type of health information may be disclosed, such as prescription history, laboratory reports, hospital encounters, and to whom.

(16) "Core elements of the Master Patient Index (MPI)" are the minimum elements that are:

(a) Required for an HIE to identify a particular patient across separate clinical, financial, and administrative systems; and

(b) Needed to exchange health information electronically.

~~(14)~~(17) "Core HIE education content" means the educational information developed and approved by the Maryland Health Care Commission, after consultation with interested parties, and includes a general overview of:

(a) The fundamentals of health information technology, including electronic health records and the exchange of electronic health information;

(b) Health information privacy and security laws; and

(c) The benefits and risks to patients of exchanging health information through an HIE as compared to opting-out and exchanging health information through a paper-based system.

~~(15)~~(18) "Covered entity"" has the meaning provided in 45 CFR §160.103.

~~(16)~~(19) "Credentialed professional" means an individual who has been credentialed by a hospital to provide clinical services to patients of the hospital. Credentialing includes the formal evaluation and verification of an individual's necessary qualifications, education, training, and professional license if applicable, through the collection, verification, and evaluation of data relevant to the individual's professional performance.

~~(17)~~(20) "Data use agreement" means an agreement that:

(a) Is entered into by an HIE and an entity receiving data for secondary data use purposes, regardless of whether or not the entity is a covered entity as defined by HIPAA; and

(b) Requires:

(i) The receiving entity to accept and comply with the requirements in this chapter and, to the extent the receiving entity meets the definition of a business associate under HIPAA, current State and federal laws pertaining to business associates and business associate agreements;

(ii) Both parties to access, transmit, and protect the PHI in accordance with current legal requirements and industry standards and practices;

(iii) The receiving entity to destroy the PHI, including back-up and archived copies of the PHI, in accordance with industry standards and practices, when the purposes for which it has been requested are completed, unless retention of the PHI is otherwise required by law; and

(iv) The receiving entity not to reuse or disclose the PHI to any person or organization, except as required or permitted by law; or if disclosed to a third party,

which will act on behalf of the receiving entity, the third party and the receiving entity enter a contractual agreement that requires the third party to be bound by the provisions of the data use agreement that applies to the receiving entity.

~~(18)~~(21) "De-identified data" means health information that neither identifies nor provides a reasonable basis to identify an individual and that meets the standards and specifications provided in 45 CFR §164.514(a)—(b).

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

(23) "Dispense" has the meaning stated in Health Occupations Article, §12–101, Annotated Code of Maryland, but does not include giving a patient prescription drug samples in accordance with Health Occupations Article, §12-102(d), Annotated Code of Maryland.

(24) Dispenser.

(a) "Dispenser" means a person authorized by law to dispense a noncontrolled prescription drug to a patient or a patient's agent in the State, including a nonresident pharmacy so authorized.

(b) "Dispenser" does not include:

(i) A licensed hospital pharmacy that only dispenses a monitored prescription drug for direct administration to an inpatient of the hospital;

(ii) An opioid treatment services program, as defined by COMAR 10.47.07.02;

(iii) A veterinarian licensed under Agriculture Article, Title 2, Subtitle 3, Annotated Code of Maryland, when prescribing controlled substances for animals in the usual course of providing professional services;

(iv) A pharmacy issued a waiver permit under COMAR 10.34.17.03 that provides pharmaceutical specialty services exclusively to persons living in assisted living facilities, comprehensive care facilities, and developmental disabilities facilities; or

~~(i)~~(v) A pharmacy issued a waiver by the Department under COMAR 10.47.07.03G from reporting dispensing to hospice patients.

~~(19)~~(25) "Download" means providing a method by which the health care consumer can obtain an electronic copy of the patient's information that:

(a) Is in a readily available industry standard format; and

(b) Allows the health care consumer to save, maintain, use, or transmit the patient's information.

(26) "Electronic health care transactions" means transactions, as defined by 45 CFR § 160.103, that meet the specifications of 45 CFR § 162.920.

~~(20)~~(27) "Electronic health information" means health information that is in an electronic form.

~~(21)~~(28) "Electronic health record" or "EHR" means an electronic record of health-related information on an individual that includes patient demographic and clinical health information that may be used for clinical diagnosis, treatment, improvement of health care quality, and patient care.

~~(22)~~(29) "Electronic health record system" means technology that electronically captures, manages, and organizes health records and may have the capacity to:

(a) Provide clinical decision support;

(b) Support physician order entry;

(c) Capture and query information relevant to health care quality; and

(d) Exchange electronic health information with and integrate the information from other sources.

~~(23)~~(30) "Emergency" has the meaning provided in Health-General Article, §4-301(d), Annotated Code of Maryland.

~~(24)~~(31) "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 health management; and

(b) Shall be minimally composed of:

(i) At least three health care consumer members, three health care provider members, one member representing the scientific community, one member with privacy and legal expertise, and one member with HIE expertise;

(ii) Members who have appropriate professional competencies necessary to review the request; and

(iii) More than half of the members are not affiliated with or related to any person affiliated with the requesting entity and are free from any conflicts of interest with the requesting entity.

~~(25)~~(32) "Federalwide assurance" or "FWA" means an agreement between an entity and the United States Department of Health and Human Services under which the entity agrees to comply with:

(a) Federal regulations concerning research involving human subjects;

(b) Department of Health and Human Services regulations found at 45 CFR Part 46;

(c) A statement of principles governing the entity in the discharge of its responsibilities for protecting the rights and welfare of human subjects of research conducted at or sponsored by the entity; and

(d) Other requirements of the agreement.

~~(26)~~(33) "Granular patient consent" means expressed preferences made by a health care consumer regarding the disclosure, access, and use of the patient's protected health information according to the type of information, type of provider, purpose, or circumstance communicated by the health care consumer to the HIE through reasonable means specified by the HIE, which shall include paper and electronic means.

~~(27)~~(34) "Health care" has the meaning provided in Health-General Article, §4-301(g), Annotated Code of Maryland.

~~(28)~~(35) "Health care consumer" or "consumer" means a recipient, a patient, or a person in interest, as defined in this regulation.

~~(29)~~ "Health care provider" has the meaning provided in Health-General Article, §4-301(h), Annotated Code of Maryland.~~means:~~

~~(30) A person who is licensed, certified, or otherwise authorized under Health Occupations Article, Annotated Code of Maryland, or Education Article, §13516, Annotated Code of Maryland, to provide health care in the ordinary course of business or practice of a profession or in an approved education or training program; or~~

~~(31) A facility where health care is provided to patients or recipients, including:~~

~~(32) A facility as defined in Health-General Article, §10101(e), Annotated Code of Maryland;~~

~~(33) A hospital as defined in Health-General Article, §19-301(f), Annotated Code of Maryland;~~

~~(34) A related institution as defined in Health-General Article, §19-301(o), Annotated Code of Maryland;~~

~~(35) A State-certified substance use disorder program, as defined in Health-General Article, §8-403, Annotated Code of Maryland;~~

~~(36) A health maintenance organization as defined in Health-General Article, §19701(g), Annotated Code of Maryland;~~

~~(37) An outpatient clinic; or~~

~~(38) A medical laboratory;~~

~~(39) An agent, employee, officer, or director of a health care facility, or an agent or employee of a health care provider.~~

(36) "Health Data Utility" means an HIE that operates for the following purposes:

(a) The collection, aggregation, and analysis of clinical information, public health data, and electronic administrative health care transactions;

(b) The communication of data between public health officials and health care providers to advance disease control and health equity; and

(c) The enhancement and acceleration of interoperability of health information.

~~(40)~~(37) "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, employer, life insurer, school or university, 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.

~~(41)~~(38) "Health information exchange" or "HIE" has the meaning provided in Health-General Article §4-301(i), Annotated Code of Maryland.

~~(42)~~(39) "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).

~~(43)~~(40) 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.

~~(44)~~(41) "HIE access matrix" means a document that is used by a participating organization to assign access to each authorized user and describes the type of protected health information (including, but not limited to, lab reports, prescription drug information, prior admissions to hospitals), that each authorized user is allowed to retrieve from an HIE. An HIE access matrix may specify a use case (including but not limited to electronic eligibility, clinical lab ordering/results delivery, electronic prescribing, medication history, clinical summary exchange, and other items) and corresponding associated data, including identified sensitive health information.

~~(45)~~(42) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, P.L.104191, as amended, and the implementing regulations at 45 CFR Parts 160 and 164, as amended, and including as amended by the HITECH Act.

~~(46)~~(43) "HITECH Act" mean the Health Information Technology for Economic and Clinical Health 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), as amended.

~~(47)~~(44) "Hospital" has the meaning provided in Health-General Article, §19-301(f), Annotated Code of Maryland.

~~(48)~~(45) "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).

~~(49)~~(46) "Institutional Review Board" or "IRB" means a committee or other group designated by an institution or affiliated with a State agency that performs a review of proposed research that has:

(a) Registered with the Office of Human Research Protections Electronic Submission System; and

(b) Obtained FWA approval from the Office of Human Research Protections.

~~(50)~~(47) "Interoperability" has the meaning provided in 45 CFR §170.102.

~~(51)~~(48) "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.

~~(52)~~(49) "Master patient index" or "MPI" means a database that maintains a unique index identifier for each patient whose protected health information may be accessible through an HIE and is used to cross reference patient identifiers across multiple participating organizations to allow for patient search, patient matching, and consolidation of duplicate records.

~~(53) "MHCC" or the "Commission" means the Maryland Health Care Commission.~~

~~(54)~~(50) "Nationally recognized standards" means technical standards for the exchange, integration, sharing, or retrieval of electronic health information considered reliable by the health IT industry nationally.

(51) "Noncontrolled Prescription Drugs" means a prescription drug, as defined in the Health Occupations Article § 21-201, that is not a controlled dangerous substance designated under Title 5, Subtitle 4 of the Criminal Law Article.

~~(55)~~(52) "Non-HIPAA violation" means an inappropriate use, access, maintenance, or disclosure of health information that is not a HIPAA violation, but is inconsistent with State or federal law or this chapter, including a violation of 42 CFR Part 2.

~~(56)~~(53) "Notice" (or "notify" or "notification") means an action that is required to be taken in writing or by written request under this chapter by a person, including an HIE, a health care consumer, a participating organization, or the ~~MHCC~~Commission, in order to provide information to another that:

(a) Is sent by letter delivered to the person's address of record;

(b) Uses one of the following electronic or digital mechanisms where the delivery is acknowledged or confirmed:

(i) An email, when the receiving person has provided an email address;

(ii) By a health care consumer using the receiver's website; or

(iii) By a health care consumer using a patient portal;

(c) By a health care consumer using telephonic or similar method, provided that a written confirmation of the conversation is provided to the health care consumer by the person receiving the notification or request by the following means:

(i) An email, when the health care consumer has provided an email address and delivery is acknowledged or confirmed; or

(ii) letter delivered to the health care consumer's address of record; and

(d) Complies with HIPAA and all other applicable federal and State laws and regulations.

~~(57)~~(54) "Opt-out" means the explicit written notice by a health care consumer to an HIE or through the consent management application that the patient has elected not to participate in the HIE, so that the HIE shall not disclose such patient's protected health information, or data derived from such patient's health information, except as consistent with this chapter.

~~(58)~~(55) "Part 2" means the federal Confidentiality of Substance Use Disorder Patient Records regulations found in 42 CFR Part 2 and supplemented by the final rule 82 FR 6052.

~~(59)~~(56) "Part 2 information" means any information subject to the regulations under 42 CFR Part 2.

~~(60)~~(57) "Participating organization" means a covered entity that enters into an agreement with an HIE that governs the terms and conditions under which its authorized users may use, access, or disclose protected health information through the HIE.

~~(61)~~(58) "Patient" means an individual who receives health care and on whom a medical record is maintained.

~~(62)~~(59) "Payor" means:

(a) An insurer that holds a certificate of authority in the State and provides health benefit plans in the State;

(b) A health maintenance organization that holds a certificate of authority in the State;

(c) A managed care organization authorized to receive Medicaid prepaid capitation payments under Health-General Article, Title 15, Subtitle 1, Annotated Code of Maryland; or

(d) A nonprofit health service plan that holds a certificate of authority in the State.

~~(63)~~(60) "Person" means an individual, trust or estate, general or limited partnership, joint stock company, unincorporated association or society, municipal or other corporation, incorporated association, limited liability partnership, limited liability company, the State, an agency or political subdivision of the State, a court, and any other governmental entity.

~~(64)~~(61) "Person in interest" means any of the following, but does not include a participating organization:

(a) An adult on whom a health care provider maintains a medical record;

(b) A person authorized to consent to health care for an adult consistent with the authority granted, including without limitation, a guardian, surrogate, or person with a medical power of attorney;

(c) A duly appointed personal representative of a deceased person;

(d) Either:

(i) A minor, if the medical record concerns treatment to which the minor has the right to consent and has consented under Title 20, Subtitle 1 of the Health-General Article, Annotated Code of Maryland; or

(ii) A parent, guardian, custodian, or a representative of the minor designated by a court, in the discretion of the attending physician who provided the treatment to the minor, as provided in Health-General Article, §§20 -102 and 20-104, Annotated Code of Maryland; or

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

(i) A parent of the minor, except if the parent's authority to consent to health care for the minor has been specifically limited by a court order or a valid separation agreement entered into by the parents of the minor; or

(ii) A person authorized to consent to health care for the minor consistent with the authority granted; or

(f) An attorney appointed in writing by a person listed in this definition regarding matters subject to this chapter.

~~(65)~~(62) "Point-to-point transmission" means a secure electronic transmission of PHI, including, but not limited to, records sent via facsimile or secure clinical messaging service, sent by a single entity that can be read only by the single receiving entity designated by the sender. A point-to-point transmission may be facilitated by an HIE and mirrors a paper-based exchange, such as a referral to a specialist, a discharge summary sent to where the patient is transferred, lab results sent to the practitioner who ordered them, or clinical information sent from a hospital to the patient's health plan for quality improvement or care management/coordination activities for such patient.

~~(66)~~(63) "Population 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) Patient outreach activities that involve care management;

(b) Development or assessment of, quality indicators, patient patterns or outcomes, or support of quality reporting;

(c) Development and evaluation of innovative care delivery models and programs; and

(d) Risk assessment.

~~(67)~~(64) "Primary use of HIE data" or "primary use" means use and disclosure of data accessed, used, or disclosed through an HIE for purposes of:

(a) Treatment as defined by HIPAA;

(b) Payment as defined by HIPAA;

(c) Reporting to public health authorities in compliance with reporting required or permitted by law;

(d) Other uses or disclosures required or permitted by law and in accordance with this chapter, including those set forth in Health-General Article, §4-305(b), Annotated Code of Maryland; or

(e) Health care operations, as defined by HIPAA, for conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical

guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities.

~~(68)~~(65) "Privacy board" means a group of individuals that:

(a) Is responsible for reviewing and making a determination on a request for secondary data for research purposes;

(b) Has the authority consistent with 45 CFR §164.512, including approval of a waiver or alteration of authorization requirement;

(c) Is designated or convened by the HIE, which may establish guidelines concerning a quorum;

(d) Shall meet the member composition requirements detailed in 45 CFR §164.512(i)(1)(i)(B)(1) and (3); and

(e) Shall assure that less than half of its members considering a request are affiliated with or related to any person affiliated with the requesting entity.

~~(69)~~(66) "Protected health information" or "PHI" a subset of health information, means:

(a) Protected health information as defined in 45 CFR §160.103; or

(b) A medical record as defined in the Health-General Article, §4-301(i); and

(c) Includes sensitive health information.

~~(70)~~(67) "Public health authority" has the meaning provided in 45 CFR §164.501.

~~(71)~~(68) "Qualified research organization" means an entity that:

(a) Has entered into a data use agreement with the HIE from which data is being requested;

(b) Is determined, by an IRB or privacy board, to have expertise to carry out research specific to its request;

(c) Is determined, by an IRB or privacy board, to have a legitimate and credible reason or obligation to carry out research specific to its request; and

(d) Is a participating organization, public health authority, or is engaged in joint research with a participating organization or public health authority.

~~(72)~~(69) "Query" means to electronically search for information available through an HIE using the services provided by the HIE.

~~(73)~~(70) "Research" means the use of secondary data available from or through an HIE for the systematic investigation, including research development, testing, preparation, and evaluation, designed to develop or contribute to generalizable knowledge as defined in 45

CFR §164.501 and 45 CFR §46.102, including the use of de-identified data and limited data sets.

(71) "Secondary use of HIE data" or "secondary use" means any use or disclosure of data accessed, used or disclosed through an HIE that is not a primary use. Examples of secondary use include, but are not limited to, use of HIE data for conducting research, improving patient safety, marketing, or the sale of HIE data.

~~(74)~~(72) "Secretary" means the Secretary of Health.

~~(75)~~(73) "Sensitive health information" means a subset of PHI, which consists of:

(a) Part 2 information;

(b) Legally protected health information; or

(c) Any other information that has specific legal protections in addition to those required under HIPAA or the Maryland Confidentiality of Medical Records Act.

~~(76)~~(74) "State ~~-designated-~~ Designated HIE" means an HIE designated by the Maryland Health Care Commission and the Health Services Cost Review Commission pursuant to the statutory authority set forth under Health-General Article, §19-143, Annotated Code of Maryland.

~~(77)~~(75) "Submit", when used in reference to consumer-submitted data, means providing a method by which the health care consumer can electronically upload information to the HIE to then be made available to authorized users of the HIE.

~~(78)~~(76) "System administrator" means an individual employee within a participating organization (or an individual employed by a contractor to the participating organization) who is designated by the participating organization to manage the user accounts of specified individuals within the participating organization in coordination with an HIE.

~~(79)~~(77) "Third party system" means hardware or software provided by an external entity to a participating organization, which interoperates with an HIE to allow an authorized user access to information through the HIE and may include an electronic health record system.

~~(80)~~(78) "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.

~~(81)~~(79) "Unusual finding" means an irregularity in the manner in which use, access, maintenance, disclosure, or modification of health information or sensitive health information transmitted to or through an HIE should occur that could give rise to a breach, a violation under this chapter or a violation of other applicable privacy or security laws.

~~(82)~~(80) "Use" has the meaning provided in 45 CFR §160.103.

~~(83)~~(81) "User accounts" mean the records associated with an authorized user's credentials and activities with an HIE or a third party system.

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

A. A health care consumer has the following rights in accordance with the requirements specified in this section:

(1) The right to have information regarding the health care consumer's rights under these regulations readily available to assist the health care consumer in making an informed decision concerning:

(a) The accessibility of a patient's protected health information electronically through an HIE; and

(b) The risks and benefits of participating in the HIE.

(2) The right to opt out of an HIE.

(a) A health care consumer has the right to opt out of an HIE at any time and refuse access to the patient's PHI through an HIE, except when a disclosure is limited to:

(i) Core elements of the MPI;

(ii) A disclosure that a person is required to make under federal or State law requirements;

(iii) Results of a diagnostic procedure sent to the health care provider who ordered the procedure or another provider as designated by the ordering provider;

(iv) Information regarding prescription medications dispensed or filled by a pharmacy, sent to the health care provider who ordered the prescriptions or another health care provider as designated by the ordering health care provider;

(v) Public health authorities for reporting purposes required, authorized, or otherwise compliant with applicable law; or

(vi) Communications permitted under HIPAA or State law without a health care consumer's consent or authorization when using point-to-point.

(b) Provided, however, that §A(2)(a)(iii), (iv), and (vi) of this regulation shall not apply to disclosures of sensitive health information, which receive additional protections consistent with Regulation .04 of this chapter.

(c) A health care consumer shall be advised in writing by the HIE receiving the opt-out notice or request that opting out does not preclude any participating organization that has received or accessed PHI via the HIE prior to such opt-out, and incorporated such PHI into its records, from retaining such information in its records.

(3) An HIE shall make a good faith effort to facilitate a health care consumer's amendment of the patient's health information available through the HIE by informing the health care consumer how to seek amendment of the information.

(a) An HIE shall send information regarding the process for amending health information being made available through the HIE within 20 days of receiving notice from a health care consumer of a

desire to amend the patient's health information available through the HIE and shall include the contact information of relevant participating organizations that provided the information; and

(b) This process shall be in accordance with the requirements specified in Health-General Article, §4-304(b), Annotated Code of Maryland and HIPAA, including 45 CFR §164.526.

(c) An HIE shall make a good faith effort to notify the participating organization of each authorized user who has accessed, used, or disclosed the health information that has subsequently been amended.

(4) The right to resume participation in an HIE after previously opting out in accordance with these regulations. Any such resumption of participation shall be upon written notice or request by the health care consumer.

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) An HIE shall develop, adopt, implement, and keep current a health care consumer education plan that considers stakeholder input.

(a) The health care consumer education plan shall include the core HIE education content as defined in Regulation .02 of this chapter.

(b) The health care consumer education plan shall outline how the HIE will make available the following information to health care consumers:

(i) A description of each type of patient health information that may be used, accessed or disclosed through the HIE;

(ii) The health information maintained by the HIE;

(iii) The specific details concerning who may access, use, or disclose a patient's health information and for what purpose;

(iv) The privacy and security measures that the HIE has implemented to protect health information, and a detailed explanation of what happens if there is a breach that results in unauthorized access to protected health information;

(v) A health care consumer's rights regarding the HIE and the control over, protection of, use of, and correction of each type of health information;

(vi) The process provided for a health care consumer to exercise the health care consumer's rights, including a detailed description of the steps a health care consumer needs to take in order to opt out from participation in the HIE;

(vii) The implications of a health care consumer's decision to opt out of participation in an HIE and not permit the disclosure of that consumer's PHI to authorized users, except as otherwise permitted under applicable law; and

(viii) The HIE's policies and procedures, including without limitation, policies and procedures consistent with these regulations regarding how the health care consumer may gain access to the patient's health information.

(2) An HIE shall develop and implement health care consumer education materials as provided in §B(1) of this regulation. Such education materials shall have the following characteristics:

(a) Provide a balanced perspective, outlining the various points of view concerning each subject matter, including the risks and benefits associated with sharing protected health information electronically through the HIE;

(b) Are not inaccurate or misleading;

(c) Minimize the use of technical terms and, when such terms are necessary, clearly define the technical terms;

(d) Use plain language that is easily understandable to each health care consumer population served, taking into account the various levels of education, understanding, and interest across that population;

(e) Use text and illustrations that are culturally sensitive, language appropriate, and that recognize user diversity including ethnicity, age, race, and gender;

(f) Update material to include and incorporate new information; and

(g) Specify the time sensitivity of any material included.

(3) An HIE shall cooperate with applicable State agencies to educate health care consumers consistent with a statewide education plan approved by such applicable State agency.

(4) An HIE shall make health care consumer educational materials readily available, at no charge, to participating organizations and 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. An HIE shall comply with the following requirements to allow a health care consumer to obtain information concerning a patient's PHI that may be available through the HIE.

(1) An HIE shall provide the following information to the health care consumer, upon written notice or request by the health care consumer, describing what PHI is available through the HIE concerning the specified patient:

(a) The participating organization that disclosed the PHI to the HIE;

(b) The date the PHI was disclosed to the HIE; and

(c) The type of PHI disclosed to the HIE, if known by the HIE.

(2) An HIE shall provide written information, in accordance with this Regulation, to health care consumers concerning the methods available to such health care consumers to access a patient's PHI that is available through the HIE.

(a) If the patient's PHI is directly available electronically to the health care consumer through the HIE, the HIE shall advise the health care consumer how to obtain the PHI electronically.

(b) If the patient's PHI is not directly available electronically to the health care consumer through the HIE, the HIE shall, within 7 days from receipt of such health care consumer's written notice or request, provide the health care consumer with the contact information for each participating organization that has disclosed information to the HIE and received information from the HIE concerning the patient, so that the health care consumer may gain access to the patient's health information directly from each participating organization.

(3) An HIE shall make a good faith effort to facilitate a health care consumer's amendment of the patient's health information available through the HIE by informing the health care consumer how to seek amendment of the information.

(a) An HIE shall send information regarding the process for amending health information being made available through the HIE within 20 days of receiving notice from a health care consumer of a desire to amend the patient's health information available through the HIE and shall include the contact information of relevant participating organizations that provided the information; and

(b) This process shall be in accordance with the requirements specified in Health-General Article, §4-304(b), Annotated Code of Maryland and HIPAA, including 45 CFR §164.526.

(c) An HIE shall make a good faith effort to notify the participating organization of each authorized user who has accessed, used, or disclosed the health information that has subsequently been amended.

(4) Upon receipt of written notice or request, an HIE shall provide each health care consumer with a report detailing any disclosure through the HIE for a time period specified by the health care consumer, of the patient's PHI. In the case of recurring disclosures to the same entity for the same purpose, a summary report may be provided by the HIE. However, if the health care consumer requests the details of the summary report, the HIE shall promptly provide them.

(a) The time period specified by the health care consumer shall not exceed the data retention period as specified in the HIPAA Privacy Rule, 45 CFR §164.528.

(b) The report shall specify the following for each instance that the patient's PHI was disclosed during the time frame reflected in the report:

(i) The name of each authorized user;

(ii) The name of the participating organization to which the authorized user is affiliated, if such information is kept by the HIE in the ordinary course of business;

(iii) The date and time of the disclosure;

(iv) The type of PHI disclosed, if known by the HIE; and

(v) The name of the participating organization that made the protected health information available to the HIE.

(c) An HIE shall acknowledge a health care consumer's written notice or request for the report within 10 business days of receipt of the request.

(d) An HIE shall respond to a health care consumer's written notice or request with either the requested report or with a written explanation why such report is unavailable, when it will be available, or where the health care consumer may obtain the requested information, in accordance with 45 CFR §164.528(a)(2)(D)(3). The HIE shall respond within a reasonable time frame, but not later than 30 days of the initial written notice or request by the health care consumer.

(i) An HIE shall provide up to two copies annually of the report at no cost to the health care consumer, upon written notice or request by the consumer. If the report is available in an electronic format, it shall be provided to the consumer in a generally available electronic format such as PDF, if so requested, at no additional charge.

(ii) For any additional report, the HIE may charge a reasonable fee not to exceed the cost to provide the additional report, but no more than the allowable amount in accordance with Health-General Article, §4-304, Annotated Code of Maryland, and 45 CFR §164.524(c)(4).

D. Consent Management Application.

(1) The State Designated HIE shall implement a consent management application that:

(a) Allows a person in interest to opt out or back into having a patient's electronic health information shared or disclosed by an HIE;

(b) Informs the person in interest of the types of electronic health information that may be shared or disclosed in accordance with §A(2)(a) of this regulation notwithstanding the choice to opt out;

(c) Enables HIEs to query whether a person in interest has opted out of or back in to sharing a patient's electronic health information;

(d) In accordance with the phases specified in §D(2)(a) of this regulation, receives and incorporates opt-out information provided by other HIEs; and

(e) At least includes:

(i) Personal identifiers consisting of the full name, date of birth, mailing address, telephone number and other unique identifiers of the patient and person in interest, if not the patient;

(ii) The person in interest's communication contact preferences;

(iv) The relationship of the person in interest to the patient; and

(v) The date the patient's consent preferences were last updated.

(2) (a) The consent management application developed by the State Designated HIE shall be implemented in three phases.

(b) Phases.

(i) Phase One. By [DATE] the State Designated HIE shall implement a register, database, or repository to serve as the consent management application that will store personal identifiers and minimally supports downloading by other HIE systems;

(ii) Phase Two. By [DATE], the State Designated HIE shall implement data feeds using industry standards recognized by a standards development organization that supports at least weekly data deliveries from the consent management application to recipient HIE systems; and

(iii) Phase Three. By [DATE], the State Designated HIE shall implement a consent management application with an application programming interface that enables a standardized way to facilitate interoperability between different recipient HIE systems.

(c) The State Designated HIE shall notify the Commission and all HIEs when each phase is functional.

(d) An HIE shall implement the technical capabilities to support Phase One of the consent management application within 60 days after notification by the State Designated HIE that the phase is functional.

(e) An HIE:

(i) May implement the technical capabilities to support Phase Two or Phase Three of the consent management application after notification by the State Designated HIE that the phase is functional; but

(ii) Shall implement the technical capabilities to support Phase Two and Phase Three of the consent management application within 90 days after direction by the Commission to implement the phase, unless the HIE demonstrates good cause to delay implementation.

(3) An HIE shall:

(a) Update the data in the HIE's system to include the most recent version of the consent management application no less than every five business days;

(b) Update the State Designated HIE's consent management application with any opt-out or opt-in requests it has received directly from a person in interest within five business days of the request;

(c) Withhold sharing or disclosure of the electronic health information of a patient to the extent the consent management application indicates that the patient has opted out of having electronic health information shared or disclosed by an HIE, except to the extent permitted by §D(2) of this regulation; and

(d) Electronically inform authorized users upon query when a patient has restricted data sharing.

(4) An HIE shall implement the consent management application in a manner that is consistent with this chapter, its existing policies and procedures regarding use and disclosure of PHI and other personal identifiable information, and its technological capabilities.

(5) An HIE shall place a link on its website directing a person in interest to the State Designated HIE's website to opt out or back into having a patient's electronic health information shared or disclosed by an HIE.

(6) The State Designated HIE shall promptly notify the Commission and all HIEs any time the consumer management application is not operational and when services are resumed.

(7) An HIE is not required to comply with §D(3) of this regulation when:

(a) An emergency exists and all requirements under Regulation .11 of this chapter have been met; or

(b) The consent management application is not operational.

~~D~~E. An HIE shall:

(1) Establish and maintain an online process that allows health care consumers to obtain an electronic report detailing any disclosures of their information through the HIE in accordance with §C(4)(b) of this regulation; and

(2) Implement and maintain compliance with the provisions detailed in Regulation .12A(1)(7), B(1)(2), and C(4)(b)(d) of this chapter in implementing §D(1) of this regulation.

F~~E~~. An HIE shall take affirmative steps to protect a patient's protected health information, including sensitive health information, that is accessible to or through the HIE from a breach or a non-HIPAA violation.

(1) An HIE shall have an easily accessible and convenient method by which a person may notify the HIE concerning a potential or an actual breach or a non-HIPAA violation.

(2) When an HIE is notified in writing of a potential or an actual breach or a non-HIPAA violation, the HIE shall:

(a) Acknowledge receipt of the notification within 1 business day;

(b) Begin an investigation concerning the matter upon receipt of the notification in compliance with Regulation .07 of this chapter and;

(c) In accordance with Regulation .08 of this chapter, provide the person filing the notification and each health care consumer whose protected health information was breached with information concerning the determination and resolution of the matter by the HIE.

(3) An HIE shall implement robust technical measures consistent with generally accepted industry best practices to assure valid patient identification and minimize patient record mismatches.

GF. An HIE shall implement a process to allow a health care consumer to make an educated decision regarding the patient's participation in an HIE, opting out from such participation, or opting to resume participation in the HIE system, in accordance with this regulation.

(1) An HIE shall maintain a log that records each patient's participation status over time; and

(a) The HIE shall retain the log for the duration required by State or federal law, whichever requires a longer retention; and

(b) The HIE shall keep the log in a retrievable storage medium.

(2) An HIE shall not disclose a patient's PHI if the health care consumer has submitted a written notice or request to opt-out of the HIE in accordance with §(A)(2) of this regulation except as otherwise permitted under applicable law and in accordance with this chapter.

(3) An HIE shall not disclose information derived from a patient's PHI, including for secondary use, if the health care consumer has submitted a written notice or request to opt-out of the HIE, except as otherwise permitted under applicable law.

(4) An HIE may not unreasonably deny a health care consumer's expressed preferences.

HG. The following requirements shall apply to all communications between an HIE and a health care consumer:

(1) An HIE shall implement a process to allow a health care consumer to communicate with the HIE about the patient's participation status through an appropriate medium of the health care consumer's choice, including the following:

(a) By telephone, via a toll-free number;

(b) By mail, via a standardized form;

(c) By fax, via a standardized form;

(d) Online, via a secure website; and

(e) In person at the HIE's offices during business hours.

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

(a) In writing;

(b) Online; or

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

(3) An HIE shall take appropriate measures to assure that a health care consumer who communicates with the HIE is authorized to act on behalf of the patient.

(4) An HIE shall implement the health care consumer's requested action within 5 business days of receipt of the health care consumer's written or online request concerning:

(a) Opting-out of the HIE; and

(b) Resuming participation in the HIE after previously opting-out.

(5) An HIE shall provide to each health care consumer the option to receive confirmation of any change in the patient's participation status. If a health care consumer requests such confirmation in writing, the HIE shall:

(a) Send the confirmation of participation status change within 3 business days of the effective date of change of such patient's participation status; and

(b) If consistent with all applicable privacy and security law and regulations, including HIPAA and applicable State law and regulations, send the confirmation of status change through one of the following methods as specified by the health care consumer:

(i) An email sent to the email address specified by the health care consumer;

(ii) A letter to an address specified by the health care consumer;

(iii) A letter by fax to a fax number specified by the health care consumer;

(iv) A letter given to the health care consumer at the HIE during normal business hours; or

(v) A text message sent to the number specified by the health care consumer.

(6) When a health care consumer changes the patient's participation status, the HIE shall provide the following to the health care consumer and, unless the patient is a minor or subject to a power of attorney or otherwise unable to handle his or her own affairs, to the patient:

(a) Information concerning when the status change will become effective; and

(b) Information concerning what information will be excluded from the HIE regarding a health care consumer who opts out.

~~H~~. A participating organization shall comply with the following requirements to assure patient and health care consumer rights.

(1) A participating organization shall inform each health care consumer no later than the first medical encounter following enrollment of the organization in an HIE, by written and oral notice, of:

(a) Such organization's participation in an HIE, including in such organization's Notice of Privacy Practices under HIPAA; and

(b) Information concerning the health care consumer's right to opt out from participation in the HIE and the process to opt out; and

(c) The types of information the participating organization will disclose to the HIE and for what purposes information accessed through the HIE may be used for treatment, payment, health care operations, and secondary use as described in this chapter.

(2) In addition to applicable HIPAA notification requirements, a participating organization shall notify each health care consumer whose protected health information, including sensitive health information, is breached or is maintained, accessed, used, or disclosed in a manner that constitutes a non-HIPAA violation in accordance with Regulation .08 of this chapter.

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

(3) 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) An HIE shall use only point-to-point transmission to allow access, use, or disclosure of the sensitive health information through an HIE, unless the HIE implements:

(a) Nationally recognized standards that support control by the health care consumer over the electronic exchange of the patient's sensitive health information consistent with the privacy and consent directives made by the health care consumer;

(b) Electronic exchange controls and processes that:

(i) Support granular patient consent for the electronic transmission of sensitive health information consistent with applicable State and federal laws concerning the access, use, or disclosure of sensitive health information, including applicable standards and technical requirements in accordance with Part 2; and

(ii) Assure that the health care consumer's granular consent controls remain associated with the sensitive health information and are adhered to as the information is transmitted through, maintained, or disclosed by the HIE; and

(c) Health care consumer educational content:

(i) That is developed and established in coordination with the Commission~~MHCC~~ and stakeholders;

(ii) That is kept current; and

(iii) The receipt of which shall be acknowledged by the health care consumer as part of the granular consent process.

(5) In the case of the improper access, use, maintenance, or disclosure of sensitive health information, including an inadvertent release through an HIE, a participating organization shall take the following actions in addition to any other requirement imposed under federal or State law:

(a) Take all steps necessary to immediately stop any further improper access, use, disclosure, or release of the patient's sensitive health information through the HIE and the improper maintenance of such information by the HIE; and

(b) In accordance with Regulation .08 of this chapter, notify each health care consumer whose sensitive health information has been accessed, used, maintained, or disclosed in violation of applicable State or federal laws, including a non-HIPAA violation.

B. Procedure for disclosing or re-disclosing of Part 2 health information.

(1) An HIE shall be in compliance with Part 2.

(2) A participating organization~~health care provider~~ that is a Part 2 program, as that term is defined by Part 2, shall identify itself as such and clearly indicate on all of its patient records any limits on use or disclosure required by Part 2.~~that such records may only be disclosed by point-to-point transmission through an HIE, if appropriate patient consent or authorization has been obtained, or as otherwise permitted by these regulations.~~

(2) An HIE or participating organization that receives Part 2 information may not re-disclose such information without appropriate patient consent or authorization except~~,~~ as permitted by applicable federal and State laws and regulations.

~~(3) A participating organization must maintain Part 2 records in accordance with applicable law.~~

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.

.05 Requirements for Accessing, Using, or Disclosing Health Information Through an HIE.

A. As a requirement of participation in an HIE, the HIE shall require each participating organization to enter into a binding participation agreement that:

(1) Requires the participating organization and each authorized user to comply with this chapter;

(2) Requires the participating organization and each authorized user to comply with all applicable federal and State privacy and security laws; and

(3) Includes a business associate agreement:

(a) In compliance with 45 CFR §164.504; and

(b) If the participating organization will maintain Part 2 information, the business associate agreement shall comply with the additional requirements that apply to a qualified service organization under 42 C.F.R. §2.11.

(4) Permits PHI disclosed through the HIE to the authorized user of a participating organization to be incorporated into the patient's medical record kept by such participating organization, and requires compliance with all applicable federal and State laws.

B. An HIE shall only disclose PHI through an HIE for a primary use consistent with the following:

(1) The disclosure shall be only to an authorized user for the specific purpose for which that authorized user is given access to the PHI; and

(2) All disclosures shall be in full compliance with these regulations.

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

D. To assure that only an authorized user accesses, uses, or discloses PHI through or from an HIE, an HIE shall:

(1) Develop and maintain an HIE access matrix that includes the defined HIE access levels available to each authorized user.

(a) The HIE access matrix shall be used for the following purposes:

(i) To assign an HIE access level to each staff member of the HIE or its contractor that allows only the minimum necessary access to PHI to perform that staff member's authorized purpose; and

(ii) To assist each participating organization and its system administrator in assigning the appropriate HIE access level to each authorized user of that participating organization.

(b) The HIE shall review its HIE access matrix annually and revise it as necessary to reflect relevant changes in technology, standards, or law; and

(c) The HIE shall have the necessary technological capabilities in its core infrastructure to limit an authorized user's access to the HIE according to the then currently assigned access level of its access matrix.

(2) Provide technical assistance and guidance to the system administrator of each participating organization in assigning the appropriate HIE access level to each of its authorized users;

(3) Comply, at a minimum, with the most recent Level 2 requirements set by the National Institute of Standards and Technology (NIST), as set forth in April 2006 in Special Publication 800-63 (Version 1.0.2): Electronic Authentication Guideline for both Registrations and for Registration Record Retention; and

(4) Adopt and implement an authentication process that:

(a) Requires the authentication of an authorized user at each "log in" prior to allowing that individual access to the HIE;

(b) Requires a single factor authentication with two characteristics that include a user name and a password, along with an additional security precaution, which may include a security question or a device registration.

(c) Ensures that the data stored in the HIE that is used to authenticate an authorized user is encrypted to the level set by industry best practices; and

(5) Accept as valid a third party system's authentication of an authorized user accessing the HIE through that third party system, as long as such access and third party system:

(a) Permits the HIE to audit and monitor the user's HIE activities; and

(b) The HIE has received written assurances from the third party system that it is compliant with these regulations and all applicable federal and State privacy and security regulations.

(6) If an HIE learns or has reason to believe that the third party system is not compliant, then it shall immediately cease acceptance of such third party system's authentication of authorized users until the third party system demonstrates compliance to the reasonable satisfaction of the HIE.

E. To assure that only an authorized user accesses, uses, or discloses PHI through or from an HIE, a participating organization shall comply with each of the following.

(1) A participating organization shall designate a system administrator who is capable of carrying out the requirements set forth in §F of this regulation on behalf of the participating organization prior to exchanging any PHI through the HIE.

(2) A participating organization shall promptly inform its system administrator of any circumstances that require any of the actions described under §F of this regulation;

(3) A participating organization shall ensure that any third party system it uses appropriately authenticates an authorized user prior to allowing that individual access to the HIE through the third party system.

(a) The third party system shall authenticate an authorized user at each "log in."

(b) The third party system shall ensure that the data stored in the system which is used to authenticate an authorized user is encrypted to the level set by industry best practices.

(c) A participating organization shall adopt and implement a protocol to be followed by a third party system that requires a user name, a password, and an additional security precaution which may include a security question or a device registration.

(4) A participating organization shall inform the HIE concerning the following:

(a) The designation of the system administrator, or any change in such designation, within 5 business days of any such designation or change;

(b) A breach or non-HIPAA violation by a person who had or has access to the HIE through the participating organization; or

(c) An act or event that it has a reasonable basis to believe is or may be a significant violation of this chapter.

F. The system administrator of a participating organization shall carry out each of the following measures on behalf of the participating organization.

(1) The system administrator shall identify each authorized user within the participating organization and shall note the individual's assigned unique user name in accordance with the most recent applicable standards issued by NIST, or other comparable standards generally adopted by the health care and HIE industry.

(2) The system administrator and HIE shall coordinate with the Commission to determine a methodology for assigning each authorized user with a unique user name and password and to assure that all HIEs use a commonly accepted protocol to avoid the possibility of duplicate user names and passwords.

(3) The system administrator, in coordination with the HIE, shall assign to each authorized user an access level that appropriately corresponds to that individual's role within the participating organization and the permitted access to PHI available through the HIE on behalf of the participating organization.

(4) The system administrator shall modify in a timely manner an authorized user's access level as appropriate to reflect any change in that individual's role within the participating organization; and

(5) The system administrator shall immediately terminate access through an HIE in accordance with Regulation .07 of this chapter for any authorized user:

(a) Who is suspended by the participating organization;

(b) Who is no longer associated with the participating organization; or

(c) Who no longer requires access to the HIE.

(6) The system administrator shall attest to the HIE regarding the appropriateness of a staff member to be an authorized user and that the HIE access level assigned to that staff member corresponds to the authorized user's role within the participating organization.

.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) Conduct each audit under this regulation in accordance with best practices using industry accepted standards and methodologies;

(3) 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, 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;

(5) Investigate each unusual finding identified in the access log audit to determine if there has been a violation of Regulation .05 of this chapter;

(6) Resolve an unusual finding by:

(a) Taking actions necessary to correct each identified technical control deficiency; or

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

(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, 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

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

(a) The HIE shall perform periodic testing to ensure that the storage medium being used will allow the data to be recovered.

(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.

(c) The data shall be kept for the longest duration of time identified in applicable State and federal requirements.

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

(1) Gathers relevant information to determine if there is a violation;

(2) Reflects the size and scope of the potential violation; and

(3) Complies with Regulation .08 of this chapter.

C. An HIE shall 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:

(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.

(3) An HIE shall provide the audit findings to the Commission in accordance with Regulation .09 of this chapter.

(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 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, 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 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 proper use and access of the HIE; and

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

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.

G. An HIE and its participating organizations shall adopt an access and auditing plan that requires the HIE and each participating organization, as applicable, to conduct a random audit of the HIE access logs on a monthly basis.

(1) The random audit included in the plan shall be assigned to the HIE or the participating organizations according to their respective system's technological capabilities.

(2) The access and auditing plan shall include:

(a) The manner used to identify a non-HIPAA violation of this chapter or a breach;

(b) The method to be used to report a non-HIPAA violation of this chapter or a breach;

(c) The reasonable steps that will be taken to promptly mitigate a non-HIPAA violation of this chapter or a breach; and

(d) A review of access logs to ensure that only an authorized user who is appropriately authenticated is granted access to HIE information through a participating organization's third party system.

(3) If a participating organization does not conduct its own audit, it shall review the HIE access logs relating to the participating organization within 10 days of receipt from the HIE. An HIE shall send HIE access logs to each participating organization no less than quarterly.

(a) The purpose of the review is to:

(i) Detect patterns of inappropriate access, use, maintenance, or disclosure; and

(ii) Compare the PHI accessed by the authorized user with the health care provided to assure that the authorized user's use of the HIE is appropriate.

(b) In order to conduct the quarterly review, the HIE shall provide a participating organization with audit record information concerning the participating organization's authorized users access of the HIE that shall include:

(i) The name and access level of each user;

(ii) The name of the patient whose PHI was accessed;

(iii) The date and time of access; and

(iv) The type of PHI that was accessed.

.07 Remedial Actions to Be Taken by an HIE.

A. An HIE shall immediately suspend a person's access to the HIE when it is necessary to avoid serious harm to the privacy or security of health information accessed, used, or disclosed through or from the HIE.

(1) An HIE may, in its sole discretion, suspend a person's access to the HIE pursuant to this section before an investigation under Regulation .07B of this chapter is completed. In addition, if the HIE determines that serious harm to the privacy or security of health information or an ongoing risk of improper use, access, maintenance, or disclosure of PHI may occur prior to conclusion of an investigation, it shall suspend a person's access to the HIE pursuant to this section before an investigation is complete.

(2) Such suspension shall continue until the underlying threat to the privacy or security of health information is contained.

B. An HIE shall conduct an investigation if there is reason to believe that a breach or non-HIPAA violation has occurred.

(1) The HIE shall begin the investigation upon learning of the allegations giving rise to a potential breach or violation.

(2) The HIE shall conduct the investigation in a thorough, timely, professional manner and take all necessary actions to gather information concerning the potential breach or violation that reflects the size and scope of such potential breach or violation.

(3) If appropriate, an investigation shall include an audit under Regulation .06 of this chapter.

(4) Upon the completion of an investigation, which shall not exceed 14 business days, an HIE shall:

(a) Make a written finding describing the results of an investigation and provide a copy to the Commission; and

(b) Maintain records of each investigation (audits, complaints, breaches, non-HIPAA violations) for at least 5 years from the date of completion of such investigation or 5 years from the date a minor patient becomes an adult, whichever is longer.

C. If an HIE has a reasonable belief that a breach or non-HIPAA violation has occurred, either as a result of an investigation or otherwise, the HIE shall:

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

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

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

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

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

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

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

(b) Each remedial action to be taken by each person and the associated time frame of the remedial action;

(c) Any action necessary to mitigate the harm that may be caused by the breach or the non-HIPAA violation;

(d) The identity of the person that is responsible for carrying out each action to mitigate harm; and

(e) Any future action that the HIE may take, including suspension of access or progressive discipline, if a person does not comply with the remedial action;

(4) Immediately suspend access of a person when one of the following occurs:

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

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

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

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

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

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

(5) 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.

D. After verifying that each remedial action is complete, an HIE may reinstate a person's authorization to access information through the HIE provided that:

(1) The Commission has not revoked the person's access to the HIE as provided in Regulation .09 of this chapter; and

(2) The HIE modifies the person's access as needed to ensure compliance with this chapter.

E. A person may file a written notice or request with the Commission that the Commission review an HIEs action under Regulation .07 of this chapter when the person has reason to believe that the HIE has acted inappropriately.

(1) A request for review shall be filed within 30 days after the person knew or had reason to know of the HIEs action in question;

(2) The request for review shall set forth each reason why the person believes that the HIE's action is inappropriate.

(3) The Commission may determine that no investigation is necessary or may take action under Regulation .09C.

F. An HIE shall provide notice of each suspension and each reinstatement of a person's authorization to access information through an HIE in the following manner:

(1) The HIE shall send an electronic notice to the person who is the subject of the action within 24 hours of the suspension or the reinstatement and to the Commission on a monthly basis.

(2) The notice shall include:

(a) The name of the person who is the subject of the action;

(b) The name of any affected participating organization;

(c) The basis for the suspension or reinstatement; and

(d) The effective date of the suspension or reinstatement.

(3) The notice shall not include PHI.

(4) The notice shall not be considered confidential.

.08 Notice of Breach and non-HIPAA Violation.

A. Notification of a breach shall be required consistent with notification requirements of applicable federal and State laws, including HIPAA and the HITECH Act.

B. When federal or State law does not require an HIE or other entity to provide notification to a participating organization or to an effected health care consumer, or when Part 2 does not mandate other notification requirements, the HIE shall provide notification of breach and, if applicable, non-HIPAA violations pursuant to this chapter.

(1) If the investigation under Regulation .07 of this chapter concluded that there was a breach or non-HIPAA violation, in addition to applicable HIPAA notification requirements, the HIE shall notify:

(a) The person who notified the HIE of the potential breach or non-HIPAA violation, if applicable, and to the extent permitted by HIPAA and other federal and State privacy laws;

(b) Any participating organization that has provided health information regarding the health care consumer involved; and

(c) Each patient or person in interest acting on behalf of each patient whose PHI or sensitive health information was inappropriately accessed or disclosed due to a breach or non-HIPAA violation.

(2) In addition to other requirements specified in this section, the HIE shall include in its notification, the contact information for the HIE, including the address and toll-free telephone number where the health care consumer can learn more information.

C. Notification to a Health Care Consumer.

(1) If the entity providing the notification under this Regulation has knowledge that another person is acting as the health care consumer for the patient, the entity shall provide the notification to that person instead of the patient.

(2) A notification to the health care consumer required under this Regulation shall be:

(a) In writing by first-class mail to the health care consumer, at the last known address of the health care consumer, if no prior election as to notice has been made; or

(b) As specified as a preference by the health care consumer under Regulation .03GF(1) of this chapter.

(3) If there is insufficient or out-of-date contact information that precludes notice consistent with this chapter, a substitute form of notice shall be provided. A substitute form of notice may include publishing the notice on the home page of the entity's website to the extent permitted by HIPAA and other federal and State privacy laws.

(4) When notice about a breach or non-HIPAA violation is required pursuant to this chapter, a participating organization or an HIE, as required, shall notify a health care consumer in writing within a reasonable time frame, but not later than 60 days from the discovery of the breach or from the date that the HIE should have reasonably discovered the breach.

(5) The written notification shall include:

(a) A description of the breach or non-HIPAA violation that occurred and the remedial actions taken by the participating organization, provided that the notification shall not contain any sensitive health information;

(b) Information about the patient's right to notify credit reporting agencies of the potential for identity theft or medical identity theft;

(c) Contact information for the HIE, including the address and toll-free telephone number where the health care consumer can learn more information;

(d) Contact information for at least one credit reporting agency;

(e) Information concerning the patient's right to opt out of the HIE; and

(f) The toll-free numbers, addresses, and websites for:

(i) The Office of the Attorney General, Consumer Protection Division; and

(ii) The U.S. Department of Health and Human Services, Office of Civil Rights.

(6) If the entity providing the notification keeps a medical record on the patient, the notification shall be placed within the patient's medical record.

D. Notification to Appropriate Authorities.

(1) Each participating organization and each HIE shall report all violations of federal or State privacy or security law to:

(a) Those federal or State authorities to which reporting such violation is required by applicable law, whether or not such laws are specifically set forth in this chapter; and

(b) Shall promptly send a copy of such report to the Commission.

(2) If the Commission is notified of a breach under this regulation, it shall forward such notification to the Office of the Attorney General, Consumer Protection Division, within 30 days after receipt of the notification.

.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) A person shall complete an application for registration in a form and manner specified by the Commission that shall include:

(a) The HIE's definition of what constitutes an unusual finding within Regulation .06 of this chapter;

(b) The HIE's current audited financial statement that demonstrates the financial viability of the HIE;

(c) The identity of the HIE's registered resident agent who shall accept service in Maryland on behalf of the HIE;

(d) Documentation showing its technical capabilities, which may include accreditation or candidacy status by a nationally recognized accrediting body; and

(e) Provisions for reasonable notice to participating organizations and the Commission if the HIE ceases to operate in Maryland; and

(f) Other information as required by the Commission.

(2) Financial Integrity.

(a) Following review of the financial statement provided by the HIE under §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) The amount of a bond, letter of guarantee, or other financial instrument required under this regulation shall be established by the Commission and be based on an HIE's financial statement.

(c) If a bond is required under §A(2)(a) of this regulation, it shall at a minimum:

(i) Identify the Commission as the sole beneficiary;

(ii) Be continuous and subject to cancellation only after 60 days' notice to the Commission;

(iii) Contain the following language or similar language acceptable to the Commission: "Payment under this bond shall be due in the event the Commission determines that the HIE is financially insolvent or unable to meet its obligations as a registered HIE in Maryland"; and

(iv) Permit the Commission to direct that the proceeds of the bond be paid or disbursed as necessary to maintain or repair the privacy and security of PHI that was or is available through the HIE.

(d) If a bond is required under §A(2)(a) of this regulation, it shall be obtained from a company licensed in the State to write surety types of insurance.

(e) If a letter of guarantee or other financial instrument is required under §A(2)(a) of this regulation, the guarantor shall submit a current balance sheet and income statement to the Commission.

(3) Within 45 days after receipt of complete information from an applicant seeking to register as an HIE in the State, the Commission shall take one of the following actions:

(a) Recognize the HIE as registered in the State; or

(b) Deny the registration for reasons enumerated to the applicant.

B. The Commission shall annually renew the registration of an HIE registered in the State that demonstrates its continued compliance with this chapter and provides the following information in a form and manner specified by the Commission, within 120 days of the close of its fiscal year:

(1) Updated information that reflects each change regarding the items in §A(1) of this regulation;

(2) Results of an audit performed in compliance with Regulation .06 of this chapter;

(3) As deemed appropriate by the Commission, additional requirements set forth in §A(2) of this regulation; and

(4) Other information as requested by the Commission.

C. The Commission may take an enforcement action against a person 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) A person shall cooperate in an investigation conducted by Commission staff into a potential violation.

(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 an investigation under §C(1) of this regulation, the Commission staff may issue a notice of proposed action that includes:

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

(b) A request for a person to submit a corrective action plan in order to achieve compliance with this chapter, which may include:

(i) An action aimed at correcting the underlying issue; and

(ii) Any other action that is appropriate under the circumstances.

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

(i) Non-public reprimand;

(ii) Public reprimand; or

(iii) Limitations on HIE registration or a person's access to information through an HIE;

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

(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.

(4) When the Commission staff determines that a notice of proposed action is not appropriate given the lack of available evidence or other circumstances, it may issue one of the following:

(a) A letter advising that no action is recommended at that time; or

(b) A letter finding that no action is warranted.

D. A person who receives a notice of proposed action from the Commission staff may request an opportunity to show cause why the proposed action should not be taken.

(1) A written request to show cause shall be filed with the Commission and shall comply with the following:

(a) It shall be filed within 20 days of the issuance of the notice of proposed action; and

(b) It shall include each fact upon which the person relies to show cause why the proposed action should not be taken.

(2) Upon receipt of a request to show cause, the Commission staff may meet with the person to attempt to resolve the matter in a manner that protects the public and is in the public interest.

(3) If a notice of proposed action is not resolved within 45 days of the filing of a request to show cause, a hearing officer shall be designated by the executive director of the Commission.

(a) The hearing officer shall hear evidence as needed;

(b) The hearing shall be conducted in accordance with the Maryland Administrative Procedure Act, State Government Article, Title 10, Annotated Code of Maryland, and these regulations.

(c) The hearing officer shall issue a recommended decision that contains proposed findings of fact and conclusions of law and may recommend that the Commission take one of the following actions:

(i) Adopt the action proposed by Commission staff;

(ii) Adopt a proposed action recommended by the hearing officer; or

(iii) Find that no action is warranted.

E. A request that the Commission not adopt the recommended decision may be made by either Commission staff or a person who is the subject of an enforcement action.

(1) Written exceptions to the recommended decision shall be filed within 20 days of receipt of the hearing officer's recommended decision.

(2) Exceptions shall specifically identify in writing each finding and conclusion to which exception is taken, citing those portions of the record on which each exception is based.

(3) A written response to exceptions to the recommended decision may be filed by an opposing party within 15 days of receipt of exceptions.

(4) Each person taking or responding to exceptions may present oral argument to the Commission, not to exceed 10 minutes per party, unless extended by the Chair of the Commission.

(5) The decision of the Commission shall be by a majority of the quorum present and voting.

F. The Commission may coordinate with the Office of Attorney General 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.

H. Exemptions.

(1) An HIE may request a 1-year exemption from certain requirements of this chapter.

(2) An exemption request must:

(a) Be in writing;

(b) Identify each specific requirement of this chapter from which the HIE is requesting an exemption;

(c) Identify the time period of the exemption, if any;

(d) State the reason for each exemption request; and

(e) Include information that justifies the exemption request.

(3) Within 45 days after receipt of complete information from an HIE requesting an exemption, the Commission shall take one of the following actions:

(a) Grant the exemption by providing written notification; or

(b) Deny the exemption request by providing written notification that enumerates the reasons for the denial to the HIE.

(4) An exemption may not be made for any requirement within this chapter that is otherwise required of the HIE by federal or other State law.

(5) An exemption may be made on the following grounds:

(a) The absence of certain functionality in the infrastructure of the HIE that does not allow the HIE to maintain compliance with the requirement;

(b) The requirement would hinder the ability of the HIE to comply with other requirements of this chapter or federal or other State laws; or

(c) The requirement would cause an undue burden or hardship on the HIE, such that the HIE would no longer be able to provide HIE services in the State.

(6) For good cause shown, the Commission may renew a 1-year exemption for an additional 1-year period.

.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.

B. Population 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 health management, if approval is obtained from an internal review committee designated by the care management organization, which has:

(a) Entered into a data use agreement with the HIE; and

(b) Attested that the request is:

(i) For population health management purposes; and

(ii) Limited to the minimum necessary to complete the function.

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

(a) The requirements of §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) The health care consumers have authorized the release of their information to the requesting entity; or

(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(4~~3~~) of this chapter; and

(c) The disclosure is consistent with the authorization.

(3) Any external and independent review committee identified by the care management organization may approve an authorization waiver request where the requesting care management organization has demonstrated that:

(a) Appropriate notice to each health care consumer was provided and no authorization or denial of authorization was received from each health care consumer within the 30-day time frame;

(b) The objectives for which the data was requested could not be met without access to the requested data; and

(c) The requested use or disclosure involves no more than minimal risk to the privacy of those health care consumers whose authorization will be waived based on the presence of attributes that include, at a minimum:

(i) An adequate plan presented to the external and independent review committee to protect PHI from improper use, storage, and disclosure in accordance with current legal requirements and industry standards and practices as determined by the external and independent review committee;

(ii) An adequate plan to destroy the PHI when the purposes for which it has been requested are completed, unless such retention is authorized under the waiver or otherwise required by law; and

(iii) Adequate written assurances that the PHI will not be reused or disclosed to any person or entity, except as authorized under the waiver, as required or permitted by law, or for authorized oversight of the use.

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

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) Requesting entity is a qualified research organization; and

(b) Requested data to be disclosed:

(i) Is for purposes related to research;

(ii) Is limited to the minimum necessary to complete the research purpose;

(iii) Will be used to serve a legitimate purpose consistent with the interest of the subject individuals; and

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

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

(a) Approval is obtained from an IRB or privacy board in accordance with 45 CFR §164.512, including documentation of waiver approval as detailed in 45 CFR §164.512(i)(2); and

(b) The IRB or privacy board has evaluated the request and confirmed that the requirements of §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 health information is to be disclosed, an HIE may only disclose individually identifiable 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 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 health information for secondary use, there shall be oversight by an IRB or privacy board for the duration of the research use.

(6) If an IRB or privacy board determines that the qualified research organization has failed to use or protect the data in accordance with the approved secondary use, the IRB or privacy board must report its findings to the HIE and the HIE must:

(a) Report the findings to federal and State agencies with jurisdiction over the violation, as deemed appropriate;

(b) Immediately terminate the data use agreement; and

(c) Direct the qualified research organization to destroy the data previously released by the HIE and attest that the data has been destroyed.

(7) The qualified research organization receiving data from an HIE for research purposes:

(a) Must contractually agree not to attempt to link de-identified data received from the HIE with other data sources in an effort to re-identify the data, or otherwise attempt in any other way to re-identify the data; and

(b) May disclose data to a third party acting on behalf of the qualified research organization only if the qualified research organization and third party enter into a data use agreement that requires the third party to be bound by the same provisions in the data use agreement between the HIE and qualified research organization.

(8) An HIE may charge a reasonable fee to a qualified research organization to which it discloses data for research, which fee must reflect the effort and be no greater than the actual direct and indirect costs required to prepare and release the data specific to the purpose authorized.

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

D. Enforcement and Reporting.

(1) An HIE is not required to take legal or equitable action to enforce the requirements of the data use agreement or of any other contractual assurance provided for in Regulation .05C of this chapter.

(2) An HIE shall make summary reports available to the public quarterly that provide specific information about requests for data for secondary use and the release of data for secondary purposes.

(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 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 health management;

(b) Require the HIE to conduct an audit of the disclosure and use of the data utilizing a third-party auditor at the expense of either the recipient of the data or the HIE, as determined by Commission;

(c) Require the receiving entity to destroy the data received and cease any further use of the data; or

(d) Prohibit an HIE from releasing data for all or certain secondary data use purposes.

(4) An HIE shall, upon the request by a health care consumer, provide an accounting of any disclosures made to a receiving entity for secondary data use purposes, in accordance with Regulation .03C(4) of this chapter.

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

A. An HIE shall develop and implement emergency access policies and procedures that satisfy the following requirements:

(1) The policies and procedures shall be included in the HIEs health care consumer education materials required by Regulation .03B(1) of this chapter; and

(2) Clearly communicate the following:

(a) The extent to which the HIE has the capability to disclose the patient's information in an emergency and how this compares to disclosure for routine access; and

(b) The circumstances under which the HIE would disclose the patient's information in an emergency, including how opting in or out of participation would impact access to the patient's information during an emergency.

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

(1) Only disclose information to the requesting health care provider if the following conditions are met:

(a) The requesting health care provider:

(i) Advises the HIE that it is the health care provider's professional opinion that an emergency exists; and

(ii) Attests that all conditions of the participating organization's policy have been met;

(b) The patient's condition preclude the participating organization from obtaining the consent of the health care consumer;

(c) Information available through the HIE may be relevant to the treatment needed by the patient in the specific emergency;

(d) The participating organization has an established policy that describes the requirements and attestation process for emergency access; and

(e) Disclosure of information available through the HIE is not in violation of applicable federal and State laws and regulations related to sensitive health information.

(2) Establish technical procedures for documenting an attestation by the requesting health care provider that the conditions in §B(1) of this regulation, were met prior to accessing information through the HIE;

(3) Review the emergency access logs at least monthly, in coordination with the participating organization, to identify any unusual finding;

(4) Take action in accordance with Regulation .06 of this chapter, in the event the emergency access log reveals an unusual finding;

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

(6) Require a participating organization to:

(a) Access only the minimum necessary information needed to care for the patient during the emergency encounter;

(b) Discontinue querying of the patient's record upon the completion of the emergency encounter;

(c) Allow emergency access only to authorized users with the appropriate access designation consistent with the policy of the participating organization; and

(d) Notify the health care consumer, as soon as reasonably possible, and no later than ten business days from the initial access, when the HIE has granted access to the health care consumer's information during an emergency.

.12 Requirements for Providing Health Care Consumers Electronic Access to Their Health Information.

A. An HIE or its third party that offers health care consumers electronic access to view, download, transmit, submit, or control their health information shall:

(1) Appropriately verify the identity of the health care consumer requesting electronic access or proposing an addition or change to the patient's information available through the HIE prior to disclosing or accepting changes to the information;

(2) Follow, at a minimum, the National Institute of Standards and Technology (NIST) Level 2 registration and identity proofing requirements as outlined in the most recent version of Special Publication 800-63: Electronic Authentication Guideline or its comparable industry best practices and may perform remote identity proofing;

(3) Implement the health care consumer's authorization for access within a maximum of 5 business days of receipt of all necessary information for identity proofing;

(4) Adopt and implement authentication processes for health care consumer electronic access that is in accordance with Regulation .05D(3) and (4) of this chapter;

(5) Establish individual unique user names and passwords in accordance with the most recent applicable standards issued by NIST, or other comparable standards generally adopted by the health care and HIE industry;

(6) Implement processes for auditing health care consumer access that are in compliance with applicable requirements of Regulation .06 of this chapter;

(7) Implement a process for suspending and reinstating a health care consumer's access in compliance with applicable requirements in Regulation .07 of this chapter;

(8) Establish processes and procedures to allow a patient to authorize an individual to have electronic access to their information;

(9) Establish processes and procedures that allow an individual to electronically access health information for a patient or patients:

(a) For whom the individual has legal authorization for such access (e.g., guardian, person with a medical power of attorney, etc.); or

(b) For whom the patient has authorized such access;

(10) Establish processes and procedures to confirm the authority of a person in interest, if not directly authorized by a patient, which must be satisfied as a condition to providing access to that person in interest; and

(11) Comply with applicable federal and State laws and regulations related to sensitive health information when disclosing such information to a health care consumer.

B. An HIE or its third party that offers health care consumers electronic access to view, download, transmit, submit, or control their information may:

(1) Charge a reasonable cost-based published fee for healthcare consumer electronic access consistent with applicable federal and State laws; and

(2) Deny a health care consumer's electronic access in accordance with:

(a) Applicable law or regulation, including 45 CFR §164.524, in coordination with applicable participating organizations; or

(b) The HIE's reasonable policies, procedures, or agreements with a participating organization and shall provide notice to the health care consumer of their right to request access to the patient's health information from the covered entity.

C. An HIE or its third party that offers health care consumer electronic access to view the patient's health information available through the HIE shall, in accordance with federal and State law:

(1) Provide the patient's health information that is equivalent to what is made available to authorized users that are health care providers, which may include:

(a) Demographic information, such as name, address, and date of birth;

(b) Provider encounters or procedures performed (e.g., hospital, ambulatory, post-acute care, etc.);

(c) Immunizations;

(d) Visit summaries;

(e) Care plan(s);

(f) Clinical test results; and

(g) Prescriptions;

(2) At a minimum, and if made available through the HIE, make the following data attributes for the patient's health information electronically available to the health care consumer:

(a) Date of the encounter, procedure, test, prescription, or immunization;

(b) Results or summary of the encounter, procedure, test, prescription, or immunization; and

(c) Source of the health information, including provider name and organization name;

(3) Inform health care consumers regarding:

(a) Contacting their health care provider to discuss the health information they may be viewing if they have any concerns or questions; and

(b) Translation services and resources that may be available, through the HIE or another entity, to help assist the health care consumer in understanding their health information; and

(4) Allow the health care consumer to view the patient's health information in an electronic format that meets the following criteria:

(a) The information is presented in substantially the same form and format as presented to an authorized user that is a health care provider;

(b) The form and format presented to a health care consumer is easy for the health care consumer to navigate;

(c) The information can be easily printed; and

(d) If supplemental information is made available along with the patient's health information, such as educational resources, the supplemental information meets the criteria specified in Regulation .03B(2)(c)—(e) of this chapter.

D. An HIE or its third party that offers health care consumers the ability to electronically control the patient's health information being made available through the HIE shall:

(1) Implement technology processes that meet industry standards and best practices and are in compliance with State and federal privacy and security laws; and

(2) Provide an electronic process by which a health care consumer can control the patient's health information that is in accordance with §C(4)(b)—(d) of this regulation.

E. An HIE or its third party that offers health care consumers the ability to download the patient's health information being made available through the HIE shall provide the patient's health information that is:

(1) In accordance with §C(3) and (4)(b)—(d) of this regulation;

(2) Requested by the health care consumer; and

(3) In a readily available industry standard format.

F. An HIE or its third party that offers health care consumers the ability to submit information to the HIE:

(1) Shall identify the source of the information, such as patient, payor, or health care provider, when presented to an authorized user of the HIE; and

(2) May not use patient submitted health information to override or replace health information submitted from other sources.

G. An HIE or its third party that offers health care consumers the ability to transmit the patients' health information being made available through the HIE to a third party of the health care consumer's designation shall comply with the requirements as detailed in:

(1) §C(3) of this regulation;

(2) §C(4)(b) and (d) of this regulation; and

(3) §E(2) of this regulation.

H. Health Care Consumer Education About Electronic Access.

(1) An HIE shall provide needed information, as part of its health care consumer education plan (as detailed in .03B(1) of this chapter and meeting the characteristics as detailed in Regulation .03B(2) of this chapter), about the services or features offered by the HIE or its third party that allows the health care consumer to electronically view, download, submit, or control the patient's information that is available through the HIE.

(2) The health care consumer education plan shall outline the process which, if available, allows a health care consumer to electronically view, download, transmit, submit, or control the patient's information that is available through the HIE, including:

(a) The information the health care consumer must provide as part of patient identity proofing;

(b) The patient's rights to:

(i) Authorize a person in interest or individual to also have access to the patient's health information; and

(ii) Request a review of a denial of access;

(c) The extent to which the health care consumer has control of the patient's health information being made available through the HIE; and

(d) The need to safeguard information obtained from the HIE to the same extent they safeguard other sensitive personal information.

.13 Noncontrolled Prescription Drugs Dispenser Reporting

A. For each noncontrolled prescription drug dispensed, the dispenser shall report drug information to the State Designated HIE in accordance with this regulation.

B. (1) The Commission shall develop a MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual.

(2) The Commission shall approve a MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual by November 1 of each year to be used for reporting in the subsequent calendar year.

(3) The MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual shall minimally:

(a) Specify the data and prescription drug information that must be submitted by dispensers to the State Designated HIE in accordance with this regulation;

(b) Specify the timeframe and frequency of data submissions to the State Designated HIE;

(c) Require a dispenser to report data elements consistent with the American Society for Automation in Pharmacy (ASAP) standards; and

(d) Include electronic reporting specifications, encryption algorithms, file layout, and the process for dispensers who are unable to submit data due to mechanical, electrical, or other technical failure.

(4) The Commission shall publish a draft Noncontrolled Prescription Drugs Dispenser Data Submission Manual on the Commission's website and in the Maryland Register at least 30 days before the public meeting at which the Commission shall consider the manual for final approval and provide at least 20 days for the submission of public comment.

(5) The Commission shall consider all comments received before final approval of the Noncontrolled Prescription Drugs Dispenser Data Submission Manual.

(6) The Commission shall publish the final MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual on its website within five days of its approval.

(7) The State Designated HIE shall post a link to MHCC's Noncontrolled Prescription Drugs Dispenser Data Submission Manual prominently on its website.

(8) The Commission may correct incomplete or erroneous information in the MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual as necessary and shall provide notice of each correction:

(a) On its website; and

(b) By email to the designated dispenser contact person.

C. Means of Data Submission and Data Format. A dispenser shall transmit noncontrolled prescription drug information to the State Designated HIE:

(1) Consistent with the requirements detailed in the most recent version of the MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual;

(2) By use of an encrypted electronic transmission method or a secure electronic reporting form; and

(3) In a format or utilizing data standards approved by the Commission.

D. Reporting Deadline.

(1) Unless granted a waiver under §F of this regulation, a dispenser shall report noncontrolled prescription drug information to the State Designated HIE, including zero reports, at least once every 24 hours.

(2) A dispenser that suffers a mechanical, electrical, or other technical failure that, as a direct consequence, precludes the dispenser's ability to report non-controlled prescription data electronically shall:

(a) Notify the State Designated HIE by a communication method approved by the State Designated HIE within 24 hours of discovery of the technical failure; and

(b) Submit a report for each noncontrolled prescription drug dispensed during the period of technical failure as soon as possible, but no later than 24 hours following reestablishment of the means of electronic reporting.

E. Acceptance and Disclosure of Noncontrolled Prescription Drug Information by the State Designated HIE.

(1) The State Designated HIE shall:

(a) Electronically collect noncontrolled prescription drug information from dispensers;

(b) Not impose any fees or other assessments on dispensers to support its operation;

(c) Make information technology necessary for dispensers to report noncontrolled prescription drug information to the State Designated HIE; and

(d) Retain noncontrolled prescription drug information collected pursuant to this section for at least five years from the date of receipt.

(2) (a) The State Designated HIE may reject data submitted dispensers that does not comply with the requirements of the MHCC Noncontrolled Prescription Drugs Dispenser Data Submission Manual.

(b) If the State Designated HIE rejects the data submitted by a dispenser, the dispenser shall correct and resubmit the data no later than three business days after receiving notification from the State Designated HIE of receipt of incomplete or inaccurate data.

(3) The State Designated HIE shall make patient-specific prescription information submitted by dispensers under this section available to health care providers for treatment, care coordination, or population health purposes.

(4) Upon written request for public health purposes, the State Designated HIE:

(a) Shall provide data collected under to this section within five days to the Maryland Department of Health, local health departments, the Commission, or the Health Services Cost Review Commission; and

(b) May provide data collected under this section:

(i) For programs led by health care providers to identify opportunities for quality improvement;

(ii) Pursuant to a court-ordered or administrative subpoena related to a case investigation of a particular dispenser, patient, or health care provider; or

(iii) For other public health purposes, as allowed by law.

F. Dispenser waiver request process.

(1) Prior to June 1, 2025, dispensers of noncontrolled prescription drug information are exempt from reporting dispensed information to the State Designated HIE.

(2) A dispenser that dispenses noncontrolled prescription drugs may seek a waiver from the Commission of the requirements in this regulation based on:

(a) Economic hardship;

(b) Technology limitations that are not reasonably within the dispenser's control;

(c) Dispensing less than 100 noncontrolled prescription drugs annually; or

(d) Other circumstances determined by the Commission to be extenuating.

(3) A request for a waiver shall be in writing and shall include:

(a) A detailed explanation of the need for the waiver;

(b) An attestation as to the accuracy of the information in the waiver request; and

(c) An attestation that the dispenser shall immediately inform the Commission if the circumstances necessitating a waiver no longer exist.

(4) Within 45 days after receipt of complete information from a dispenser requesting a waiver, the Commission shall:

(a) Grant the waiver request; or

(b) Deny the waiver request, with an explanation that enumerates the reasons for the denial.

(5) A dispenser shall inform the Commission and immediately begin reporting in compliance with this section if the dispenser no longer meets the conditions of a waiver request.

.14 Operation of the State Designated HIE as a Health Data Utility

A. The State Designated HIE shall operate as a health data utility for the State.

B. The State Designated HIE shall implement a consent management application in accordance with Regulation .03D.

C. Disclosures by the State Designated HIE.

(1) Except as otherwise prohibited under this chapter or State or federal law, the State Designated HIE shall transmit clinical information or electronic health care transactions to the Maryland Department of Health, the Health Services Cost Review Commission, or to the Commission for public health purposes upon written request.

(2) The State Designated HIE may not redisclose financial information in electronic health care transactions it receives in accordance with COMAR 10.25.07.09 to any person other than the Commission.

(3) The State Designated HIE shall:

(a) Develop a process in which requests for data are submitted and data are shared, and post this information on its website; and

(b) Provide a written explanation for a denial of a request which shall include an appeal process.

(3) The State Designated HIE shall consult with the Maryland Department of Health, the Commission, and Health Services Cost Review Commission before identifying any specific purposes, type of data exchanged, and rules for interaction between users and the State Designated HIE pertaining to:

(a) A State health improvement program;

(b) Mitigation of a public health emergency;

(c) Improvement of patient safety; and

(d) Any other public health priorities identified by the Secretary.

D. Consumer Advisory Council.

(1) The State Designated HIE shall establish a Consumer Advisory Council in accordance with Health-General, § 19-145, Annotated Code of Maryland.

(2) The State Designated HIE shall:

(a) Appoint a consumer representative identified by the Commission that has significant experience in public health and patient privacy as one of the council's members;

(b) Post advance notice of council meetings on its website, including an expected agenda;

(c) Make the Consumer Advisory Council meetings available to the public; and

(d) Post a recording or a transcript of every Consumer Advisory Council meeting on its website within 5 days of the meeting.