The MARYLAND
HEALTH CARE COMMISSION

Title 10 DEPARTMENT OF HEALTH AND MENTAL HYGIENE

Subtitle 25 MARYLAND HEALTH CARE COMMISSION

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

DRAFT AMENDMENTS FOR INFORMAL PUBLIC COMMENT

Comments Due October 16, 2015

The Maryland Health Care Commission (MHCC) was given the authority under Md. Code Ann., Health-Gen. §§4-301 and 4-302, signed into law on May 19, 2011, to adopt regulations for the privacy and security of protected health information obtained or released through a health information exchange. The regulations, COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information, went into effect in March 2014. This working document serves as a draft of amendments to the regulations and is no way final. The MHCC is seeking informal public comment to the draft amendments herein only. Please note amendments are either added language in italics, or deletions in brackets. Informal public comments will be accepted in writing by 5pm on October 16, 2015 and may be submitted via mail to the MHCC Attn: Christine Karayinopulos, Center for Health Information Technology and Innovative Care Delivery, 4160 Patterson Ave., Baltimore, MD 21215; or via email to christine.karayinopulos@maryland.gov.

Table of Contents

Title 10

DEPARTMENT OF HEALTH AND MENTAL HYGIENE

Subtitle 25 MARYLAND HEALTH CARE COMMISSION

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

Authority: Md. Code Ann., Health-Gen. §§19-101, 19-143, 4-301 and 4-302.2

Annotated Code of Maryland

.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 the State-Designated *health information exchange (*"HIE*")* that will assist public health agencies in reaching public health goals.

B. This chapter applies to:

(1) A health information exchange, as defined in Regulation .02*B*(17) of this chapter;

(2) A person who accesses, uses or discloses protected health information through a health information exchange; and

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

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; or

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

(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. The requirements in this chapter are in addition to those required by:

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

(2) The Maryland Consumer Protection Act, Maryland Commercial Law Article §13-101 et seq.;

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

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

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

(6) 42 CFR § Part 2 regulations; and

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

.02 Definitions.

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

B. Terms Defined.

(1) "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) "Appropriate notice to consumers" means a written notice related to a request for identifiable data that meet 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 consumers;

(iii) Must include a clear and detailed description of the steps a 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 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 as detailed in Regulation .03B(2)(b-g) of this chapter.

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

(i) Written notice as described above, making at least three attempts using varied methods to reach the consumer;

(ii) Various methods for submitting an authorization or denying authorization, such as email, online, mail, and phone; and

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

(3) "Authorization" has the meaning stated in 45 C.F.R. § 164.508.

[(2)] *(4)* "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(s) and whose HIE access is not currently suspended or terminated under Regulation .05, .07, or .09 of this chapter.

[(3)] *(5)* "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:

1. With a need-to-know; and

2. Who are under a confidentiality restriction, which may include a binding work force policy and procedure.

[(4)] *(6)* "Authentication" means the process of establishing confidence in user identities electronically presented to an information system.

[(5)] *(7)* "Breach" has the meaning as [defined in HIPAA, as amended by the HITECH Act] *stated in 45 C.F.R. § 164.402*.

[(6)] *(8)* "Business associate" has the meaning as [defined] *stated* in 45 CFR §160.103.

[(7)] *(9)* "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.

(10) "Care management organization" means any entity that:

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

(b) Has a contractual or other relationship with a State or Federal government or agency that provides them with the above mentioned responsibility; or

(c) Is under a legal or regulatory role that provides them with the above mentioned responsibility.

[(8)] *(11)* "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 [instead of] exchanging health information through a paper-based system.

[(9)] *(12)* "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.

[(10)] *(12)* "Covered entity" has the meaning as [defined] *stated* in 45 CFR §160.103.

(14) "Data use agreement" means an agreement that:

(a) Is entered into by an HIE and the care management organization or qualified research organization 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 current state and federal laws pertaining to Business Associates and Business Associates agreements;

(ii) Both parties to properly transmit, secure, and protect the PHI in accordance with current legal and regulatory requirements, and/or industry standards and practices;

(iii) The receiving entity to securely destroy the PHI 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 other person or entity, except:

1. As required or permitted by law; or

2. If disclosed to a third party, which will act on behalf of the organization, and a contractual agreement is entered into between the third party and the care management organization, where the provisions of data use agreement which apply to care management organization also apply to the third party.

(15) "De-identified data" means:

(a) Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual; and

(b) Meets the standards and specifications as detailed in 45 CFR §164.514(a)-(b).

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

[(12)] *(17)* "Electronic health record *("EHR")*" [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.

[(13)] *(18)* "Electronic health record system" means technology that [is certified by an agency of the federal government or its designated body] *electronically captures, manages, and organizes health records* and [has] *may have* the capacity to:

(a) [Manage and organize electronic health records;

(b)] Provide clinical decision support;

[(c)] *(b)* Support physician order entry;

[(d)] *(c)* Capture and query information relevant to health care quality; and

[(e)] *(d)* Exchange electronic health information with and integrate the information from other sources.

(19) "Emergency" has the meaning stated in Health-General Article §4-301(d), Annotated Code of Maryland

(20) "External and independent review committee" means a group of individuals that:

(a) Is responsible for reviewing and making a determination regarding requests for a waiver of authorization related to population care management; and

(b) Must be minimally composed of:

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

(ii) Members that 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.

(21) "Federalwide Assurance ("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 45 CFR Part 46; and

(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.

[(14)] *(22)* "Health care consumer" means a patient or a person in interest, as defined herein.

[(15)] *(23)* "Health care provider" means:

(a) A person who is licensed, certified, or otherwise authorized under the Health Occupations Article, *Annotated Code of Maryland*, or §13–516 of the Education Article, *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

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

(i) A facility as defined in Health-General Article §10–101(e), Annotated Code of Maryland;

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

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

(iv) A State-certified [alcohol and drug treatment] *substance use disorder* program, as defined in Health-General Article §8-403;

(v) A health maintenance organization as defined in Health-General Article §19–701(g), Annotated Code of Maryland;

(vi) An outpatient clinic; or

(vii) A medical laboratory.

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

[(16)] *(24)* "Health information" means any information, whether oral or recorded in any form or medium, 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.

[(17)] *(25)* "Health information exchange *("HIE")*" [or "HIE"] means an entity that creates or maintains an infrastructure that provides organizational and technical capabilities in an interoperable system for the electronic exchange of protected health information among participating organizations not under common ownership, in a manner that ensures the secure exchange of protected health information to provide care to patients. An HIE includes a payor

HIE but does not include an entity that is acting solely as a health care clearinghouse, as defined in 45 CFR §160.103. A payor may act as, operate, or own an HIE subject to these regulations.

[(18)] *(26)* "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.

[(19)] *(27)* "HIPAA" means the [U.S.] Health Insurance Portability and Accountability Act of 1996, P.L.104-191, as [implemented and] amended*, and the implementing* [in federal] regulations[, including the HIPAA Privacy and Security rules, 45] *at 45* CFR *Parts* [§§]160 and 164, as [may be] amended, [modified, or renumbered] and including as amended by *the* HITECH Act.

[(20)] *(28)* "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 [implemented and] amended [in federal regulations].

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

(30) "Identifiable data" means any health information that includes personal identifiers, as detailed in 45 CFR 164.501.

(31) "Institutional Review Board ("IRB")" means a committee or other group designated by an institution and 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.

[(22)] *(32)* "Master patient index *("MPI")*" [or "MPI"] means a database that maintains a unique index identifier for each patient whose protected health information may be accessible through the 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.

[(23)] *(33)* "MHCC" or the "Commission" means the Maryland Health Care Commission.

[(24)] *(34)* "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.

[(25)] *(35)* "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, 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) A 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.

[(26)] *(36)* "Opt-out" means the explicit written notice by a health care consumer to an HIE 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.

[(27)] *(37)* "Part 2" means the federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations found in 42 CFR Part 2.

[(28)] *(38)* "Part 2 information" means any information subject to the regulations under 42 CFR Part 2.

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

[(30)] *(40)* "Patient" means an individual who receives health care and on whom a medical record is maintained.

[(31)] *(41)* "Payor" means an entity that has a valid certificate of authority issued by the Maryland Insurance Commissioner.

[(32)] *(42)* "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.

[(33)] *(43)* "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 subsection (d) of this subsection 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.

[(34)] *(44)* "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.

(45) "Population care management purpose" means the use of data available from or through an HIE for population-based activities relating to improving patient and population health or reducing 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/programs; and

(d) Risk assessment.

[(35)] *(46)* "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 disclosure 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.

(47) "Privacy Board" means a group of individuals that:

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

(b) Has the same 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; and

(d) Must meet the member composition requirements as detailed in 45 CFR § 164.512(i)(1)(i)(B)(1) and (3), and more than half of the members must not be affiliated with or related to any person affiliated with the requesting entity.

[(36)] *(48)* "Protected health information *("PHI")*", [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.

[(37)] *(49)* "Public health authority" has the meaning provided in 45 CFR §164.501.

(50) "Qualified research organization" means any entity that has:

(a) 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; and

(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.

[(38)] *(51)* "Query" means to electronically search for information available through an HIE using the services provided by the HIE.

(52) "Research" means the use of 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 42 CFR § 164.501 and 45 CFR § 46.102, including the use of de-identified data and limited data sets.

[(39)] *(53)* "Secondary use of HIE data" or "secondary use" means any use [and] *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.

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

(a) Part 2 information; or

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

[(41)] *(55)* "State-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.

[(42)] *(56)* "System administrator" means an individual employee within a 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.

[(43)] *(57)* "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.

[(44)] *(58)* "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.

[(45)] *(59)* "Use" has the meaning provided in 45 CFR §160.103.

[(46)] *(60)* "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 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 patient's consent or authorization when using point-to-point.

(b) Provided, however, that subsections (a) (iii), (iv), and (vi) above 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) The right to the additional protections to and restrictions for disclosure of a patient's sensitive health information provided by State or federal law and consistent with Regulation .04 of this chapter.

(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 above in subsection [§]B(1) of Regulation .03. 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 to participating organizations and their users.

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 seven 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 facilitate the correction of inaccurate health information available through the HIE by informing the health care consumer how to correct perceived inaccurate information.

(a) An HIE shall send information regarding correction of health information within 20 days of receiving notice from a health care consumer of a potential inaccuracy in the patient's health information available through the HIE and shall include the contact information of relevant participating organizations that provided the perceived inaccurate information; and

(b) This process shall be in accordance with the requirements specified in 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 corrected.

(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. 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 [one (1)] *three (3)* business day;

(b) Begin an investigation concerning the matter within [two] *five (5)* business days of 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.

E. 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 Regulation .03.

(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 both applicable State and federal law; 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 Regulation .03(A)(2) 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.

F. 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 in:

(a) 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 .03F(5)(a)-(b).

(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 five 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 three 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.

G. 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, and health care operations.

(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 accessed, used, maintained, 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 but not limited to 42 CFR Part 2, concerning the access, use, or disclosure of sensitive health information through an HIE and maintenance of such information by an HIE. Until the Commission issues regulations governing the access, use, or disclosure of sensitive health information through an HIE or maintenance of such information by an HIE, all sensitive health information shall only be transmitted via point-to-point transmission.

(2) If federal or State law requires written consent or authorization for access, use, or disclosure of sensitive health information, a person shall:

(a) 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; and

(b) Use only point-to-point transmission to allow access to, use, or disclosure of the sensitive health information through an HIE.

(3) Notwithstanding subsection (2)(a) above, an HIE may transmit sensitive health information via point-to-point transmission:

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

(b) In an emergency, as defined by Health-General Article §4-301(d), if a health care provider makes a professional determination that an immediate disclosure is necessary to provide for the emergency health care needs of a patient or recipient.

(4) 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) A health care provider that is a Part 2 program shall identify itself as such and clearly indicate on all of its patient records 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) A participating organization that receives Part 2 information may not re-disclose such information without appropriate patient consent or authorization, or as otherwise permitted by these regulations.

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

.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. [Secondary use of HIE data. Until regulations regarding the secondary use of HIE data have been adopted by the Commission:

(1) Secondary use of data is permitted only for population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, and contacting health care providers and patients to provide information about treatment alternatives; and

(2) Data for secondary use may not be sold for financial or other remuneration.]

[D.] 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.

[E.] *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.

[F.] *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 Regulation .05G of this chapter 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 Regulation .05G;

(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 five 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.

[G.] *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.

(2) Each audit under this Section .06 shall be performed in accordance with best practices using industry accepted standards and methodologies;

(3) [At least monthly, c]*C*onduct [a random] audit*s* of the user access logs *on a near real-time basis* to identify any unusual finding[; and, if the HIE has been notified about an unusual finding or has reason to believe that inappropriate access has occurred, more frequently than monthly].

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

(5) Resolve the matter surrounding 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.

(6) Report any unusual finding to each participating organization involved in the unusual finding as follows:

(a) If the unusual finding involves fewer than 10 patients, in a timely manner;

(b) If the unusual finding involves between 10 and 50 patients, within two business days;

(c) If the unusual finding involves more than 50 patients, within one business day; and

[(d)] *(7)* Maintain an audit trail of user access logs in a retrievable storage medium.

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

[(ii)] *(b)* 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 violation of this chapter, the HIE shall conduct an unscheduled audit that shall:

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

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

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

C. An HIE shall conduct an annual privacy and security audit in compliance with the following provisions.

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

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

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

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

(1) Provide the results of any audit that is required by this chapter, and any supporting documentation; and

(2) Conduct an additional unscheduled audit 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 violation of this chapter, or if the health information of more than ten patients was improperly used, accessed, maintained, or disclosed during the 12 months prior to the audit, then:

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

(a) Educate and train a participating organization or an authorized user on proper access, use, and disclosure of information through or from the HIE, as appropriate; or

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

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

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

F. 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*s* of the HIE access logs on a [monthly] *near real-time* 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 consumer 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 as soon as practicable but no later than [the next] *five (5)* business day after 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 five years from the date of completion of such investigation or five years from the date a minor patient becomes an adult, whichever is longer.

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

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

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

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

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

(a) A copy of the findings of the investigation, excluding any 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 person that is responsible for carrying out each action to mitigate harm; and

(e) Any future action that the HIE may take, including suspension, if the person does not comply with the remedial action.

(3) The HIE shall immediately suspend access for an authorized user or participating organization when one of the following occurs:

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

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

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

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

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

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

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

D. 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 HIE's 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 HIE's 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 [and to the Commission] 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 Section .03 F. (1).

(3) If there is insufficient or out-of-date contact information that precludes notice consistent with these Regulations, 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 Regulation .09A(1) of this chapter, 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 [an] *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 [30] *120* days of the close of its fiscal year:

(1) Updated information that reflects each change regarding the items in subsection A(1)

(2) Results of an audit performed in compliance with Regulation .06 of this chapter [that shows that the HIE remains financially viable];

(3) As deemed appropriate by the Commission, additional requirements set forth in subsection A(2); and

(4) Other information as requested by the Commission.

C. The Commission may take an enforcement action against a person where 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.

(2) After needed investigation, the Commission staff may issue a notice of proposed action that includes the following:

(a) The details regarding each potential violation;

(b) The corrective action plan, if any, that the Commission staff recommends, which may include any of the following:

(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 registration or a person's access to information through an HIE; or

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

(3) 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 [implemented] *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, Consumer Protection Division concerning any potential violation involving a matter within the Attorney General's authority pursuant to State or federal law.

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

A. Population care management.

(1) An HIE may disclose de-identified data or a limited data set to a care management organization for purposes related to population care 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 care management purposes; and

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

(2) An HIE may disclose identifiable data to care management organizations for purposes related to population care management, if:

(a) Requirements under Regulation .10A(1)(a) and (b) of this chapter are met; and

(b) Appropriate notice has been provided to consumers whose information is being requested;

(i) The 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 consumers who were provided appropriate notice, in accordance with Regulation .02B(2) 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 care management organization has demonstrated that:

(a) Appropriate notice to the consumer was provided and no authorization or denial of authorization was received from the consumer within the 30 day timeframe;

(b) The objectives for which the data was requested could not be met without access to the requested data, as determined by a qualified member of the external and independent review committee; and

(c) The requested use or disclosure involves no more than minimal risk to the privacy of those consumers whose authorization will be waived based on at least the presence of:

(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 and regulatory requirements, and/or 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 other person or entity, except as authorized under the waiver, as required or permitted by law, or for authorized oversight of the use.

B. Research

(1) An HIE may disclose de-identified data to a qualified research organization for research purposes if the 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 identifiable data 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 164.512(i)(2); and

(b) The IRB or Privacy Board has evaluated and confirmed that the requirements of Regulation .11B(1)(a) and (b)(i-iii) are met.

(3) If an IRB or Privacy Board does not waive or alter the requirement of authorization from consumers whose identifiable data is to be disclosed, an HIE may only disclose identifiable data of 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 identifiable data may only be made if consumer authorization is obtained.

(5) As part of an HIE's Data Use Agreement with an entity to which it disclosed identifiable data for secondary use, there must 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 entity 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 entity 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) That receives de-identified data, must contractually agree to not attempt to link data received with other data sources in an effort 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 comply with 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 must be reflective of the effort and recovers the actual direct and indirect costs required to prepare and release the data specific to the purpose authorized.

C. 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 will 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, pertaining to the release of information for population care management. The Commission may:

(a) Require a care management organization to provide additional information as it relates to their use of data from an HIE for population care management for review by the Commission or a designated third party;

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

(c) Require the receiving party 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 provide a health care consumer, upon request an accounting of any disclosures made to an entity for secondary data use purposes, in accordance with Regulation .03 C(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 meet the below requirements.

(1) The policy must be included in their consumer education materials as provided in 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 consumer's information in an emergency versus 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 HIE's emergency access policy allows the disclosure of information during an emergency, the following requirements must be met.

(1) An HIE shall only disclose information to the requesting health care provider if the following conditions are met:

(a) In the professional opinion of the requesting health care provider, an emergency exists;

(b) The consumer's condition precludes the ability for the participating organization to obtain consumer consent;

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

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

(e) The requesting health care provider has attested that all conditions of the participating organization's policy have been met.

(2) An HIE shall:

(a) Establish technical procedures for documenting an attestation by the requesting health care provider that the above conditions, under Regulation.11 B(1)(a-e) of this chapter, were met prior to accessing information through the HIE;

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

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

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

(e) Require participating organizations to:

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

(ii) Discontinue querying of the consumer record upon the completion of the emergency encounter;

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

(iv) Notify consumers, as soon as reasonably possible, and no later than 10 business days from the initial access, when their information has been accessed through the HIE during an emergency.