The MARYLAND HEALTH CARE COMMISSION

# *Health Information Exchange During a State of Emergency*

## A Guidance Document for Health Information Exchanges

## February 2019

---

## Introduction

The Maryland Health Care Commission's (MHCC) Health Information Exchange Policy Board, a staff advisory group, has developed policy guidelines for a Health Information Exchange (hereafter referred to as an HIE services provider) to enable secure and appropriate exchange of protected health information (PHI) during a state of emergency. This policy guidance document aims to assist an HIE services provider that is considering making PHI accessible to incident responders during a state of emergency. *An HIE services provider should use the guidelines to inform the development and implementation of a state of emergency HIE access policy.*

In a state of emergency, such as a catastrophic weather event or public health crisis, individuals may receive care outside of their usual facilities or provider networks. When an area's health care system is strained during a disaster, incident responders are activated. When incident responders have access to a patient's health information through an HIE, they are enabled to provide more effective and timely medical care. Access to an HIE may also assist with coordination of family reunification and other notification activities. Included in this policy guidance document are key elements of a framework that facilitates the availability of PHI through an HIE services provider.

## Relevant Maryland Regulations

**COMAR 10.25.18, Health Information Exchanges: Privacy and Security of Protected Health Information (unofficial extract below):**

> 10.25.18.03 *Rights of a Health Care Consumer Concerning Information Accessed, Used or Disclosed Through an HIE*. 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 disclosure is limited to core elements of the Master Patient Index (MPI); a disclosure that a person is required to make under federal or State law requirements; results of a diagnostic procedure sent to the health care provider who ordered the procedure or another provider as designated by the ordering provider; information regarding prescription medications dispensed or filled by a pharmacy, sent to the health care provider who ordered the prescriptions or another provider as designated by the ordering health care provider; public health authorities for reporting purposes required, authorized, or otherwise compliant with applicable law; or communications permitted under HIPAA or State law without a consumer's consent or authorization when using point-to-point. 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.
>
> 10.25.18.05 *Requirements for Accessing, Using, or Disclosing Health Information Through an HIE*. To assure that only an authorized user accesses, uses, or discloses PHI through or from an HIE, an HIE shall develop and maintain an HIE access matrix that includes the defined HIE access

levels available to each authorized user; 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; adopt and implement an authentication process; and accept as valid a third party system's authentication of an authorized user accessing the HIE through that third party system.

10.25.18.06 *Auditing Requirements*. To ensure that only an authorized user who is appropriately authenticated is granted access to HIE information, an HIE shall develop and implement protocols, methodologies, and a monitoring approach designed to discover any unusual findings, which may be identified within an audit of the user logs, including conducting ongoing electronic monitoring of user access logs and investigate any unusual findings in accordance with this chapter; conduct each audit under this regulation in accordance with best practices using industry accepted standards and methodologies; investigate any unusual finding identified in the access log audit to determine if there has been a violation of Regulation .05 of this chapter; resolve the matter surrounding an unusual finding and report the unusual finding to each participating organization involved in the unusual finding; and maintain an audit trail of user access logs in a retrievable storage medium. When an HIE has identified a potential violation of this chapter, the HIE shall conduct an unscheduled audit that shall gather relevant information to determine if there is a violation; reflect the size and scope of the potential violation; and comply with Regulation .08 of this chapter.

## Relevant Federal Law

### Health Insurance Portability and Accountability Act of 1996 (HIPAA)

**45 CFR 164.502:**

*(a)(1)(ii) A covered entity is permitted to use or disclose protected health information for treatment, payment, or health care operations, as permitted by and in compliance with §164.506.*

**45 CFR 164.506:**

*(c)(2) A covered entity may disclose protected health information for treatment activities of a health care provider.*

**45 CFR 164.510(b):**

*(4) Uses and disclosures for disaster relief purposes. A covered entity may use or disclose protected health information to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b)(1)(ii) of this section. The requirements in paragraphs (b)(2), (b)(3), or (b)(5) of this section apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.*

*(b)(1)(ii) A covered entity may use or disclose protected health information to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of protected health information for such*

*notification purposes must be in accordance with paragraphs (b)(2), (b)(3), (b)(4), or (b)(5) of this section, as applicable.*[1,2]

## Policy Guidance

HIE services providers that choose to allow incident responders access to the HIE during a state of emergency should have in place organizational policies that reasonably protect the privacy and security of PHI. The following policy guidelines should be considered by HIE services providers. These guidelines apply specifically to permitted purposes and permitted users to access information in a state of emergency, for a specific time period necessary to address patient needs; all other policies remain in place.

- Access to PHI for appropriately credentialed incident responders through collaboration with an established third party registry, such as the Maryland Responds Medical Reserve Corps (MRC), American Red Cross, or other similarly vetted program, or through confirmation of certification qualifications of individuals who are temporarily designated as incident responders;
- Advanced establishment of policies and procedures related to appropriate critical operations, such as enrollment procedures, user requirements, pre-approvals, and system training with considerations for on-site registration of incident responders, as necessary;
- Establishment of time limits of authorization for incident responder access ;
- Assignment of appropriate incident responders' role-based user access levels;
- Required authentication (e.g., user name and password) of incident responders at each log in;
- Disclosure of patient information to incident responders for the following purposes:
    - Treatment, as defined by HIPAA;
    - Coordinating the notification of family members or other persons involved in the patient's care, of the patient's location, general condition, or death; and
    - Preventing or lessening a serious and imminent threat to the health and safety of a person or the public consistent with the provider's standards of ethical conduct;[3]
- Access to patient information for incident responders that is not limited to an established treatment relationship prior to the state of emergency; and
- Auditing of access and disclosures by incident responders in compliance with audit requirements under HIPAA and COMAR 10.25.18.06 *Auditing Requirements*.

[1] 45 CFR 164.510 available at: https://www.law.cornell.edu/cfr/text/45/164.510.
[2] U.S. Department of Health and Human Services, Office of Civil Rights. Bulletin: HIPAA Privacy in Emergency Situations. November 2014. Available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/emergency/hipaa-privacy-emergency-situations.pdf.
[3] 45 CFR 164.512(j) available at: https://www.law.cornell.edu/cfr/text/45/164.512.

## Definitions

Covered entity – health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which the U.S. Department of Health and Human Services (HHS) has adopted standards.

Health care provider – as defined in COMAR 10.25.18.02B, a person who is licensed, certified, or otherwise authorized under the Health Occupations Article, Annotated Code of Maryland, or Education Article, §13-516, 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.

Incident responder – an individual that has been activated for service in response to a state of emergency and participates in an established incident responder registry such as the MRC, or is a registered volunteer of a disaster-relief organization (e.g., the American Red Cross).

Incident responder registry – a database that includes health care providers licensed in Maryland under the Health Occupations Article to provide health care and who are incident responders.

Protected health information – as defined in COMAR 10.25.18.02B, a subset of health information as defined in 45 CFR §160.013, or a medical record as defined in the Health-General Article, §4-301(i), and includes sensitive health information.