Craig P. Tanio, M.D.
CHAIR

MARYLAND HEALTH CARE COMMISSION

Ben Steffen
EXECUTIVE DIRECTOR

Health Information Exchange: Maryland Privacy and Security Regulations

Overview

The Maryland Health Care Commission (MHCC or Commission) adopted regulations, as required by law, for the privacy and security of protected health information (PHI)[1] exchanged through a health information exchange (HIE).[2] The regulations aim to ensure that electronic health information is private and secure, while facilitating the use of the information to improve patient care and population health. The regulations were developed in coordination with stakeholder input over several years and went into effect on March 17, 2014.

Definition of an HIE

An HIE is considered an entity that provides organizational and technical capabilities for the secure electronic exchange of PHI among providers across health care organizations. There are currently three key forms of health information exchange:

- Direct Exchange, which has the ability to send and receive secure information electronically between care providers to support coordinated care
- Query-based Exchange which has the ability for providers to find and/or request information on a patient from other providers, often used for unplanned care
- Consumer Mediated Exchange which has the ability for patients to aggregate and control the use of their health information among providers

The goal of the electronic exchange of health information is to facilitate access to and retrieval of patient information to provide safer, timelier, efficient, effective, and patient-centered care.

Goals of the Regulations

- Assure the privacy and security of PHI accessed and or used through an HIE;
- Improve access to clinical records by treating providers; and
- Promote uses of HIE that will support public health goals.

Key Provisions of the Regulations

The regulations detail the administrative and technical requirements of HIEs and include provisions for organizations and individuals exchanging PHI through HIEs as summarized below.[3]

Consumer Rights

Consumers must be provided with an opportunity to choose not to participate in HIEs, including information concerning who has accessed their health information. HIEs and those organizations participating with HIEs must enable consumer rights, such as:

- Participating organizations must inform consumers of its participation in an HIE and the consumer's right to opt out at any time from having their PHI exchanged in an HIE;
- HIEs must provide information relating to health information that has been requested through the HIE to a consumer whose PHI may be accessed used, or disclosed through the HIE;
- HIEs must develop and make available consumer education materials to inform consumers about their rights and provide information to assist consumers in making informed decisions about their participation with an HIE.

[1] Under the HIPAA Privacy Rule, PHI refers to individually identifiable health information.
[2] COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information*.
[3] A complete list of requirements are outlined in COMAR 10.25.18. Organizations that use services of an HIE are defined as participating organizations.

Access, Use, or Disclosure of PHI

HIEs shall take steps to protect a consumer's PHI, including sensitive health information,[4] that is accessible through the HIE from any inappropriate access or use. HIEs must put in place procedural and technical controls, including authorization and consent from the consumer, consistent with applicable federal and State law. Sensitive health information may only be exchanged electronically using a secure message or email through an HIE. Use of the data from an HIE is only permitted for:

- Treatment, payment and certain health care operation purposes;
- Reporting to public health authorities as required in law; and
- Population level data requests.

Auditing Requirements

Auditing requirements for HIEs aim to ensure that appropriate controls are in place and maintained by an HIE and that HIEs take action when they suspect inappropriate accesses of PHI.

- At least monthly, an HIE must conduct random audits of user access to the HIE, and promptly investigate any unusual findings identified;
- When an HIE has identified a potential violation, the HIE shall conduct an unscheduled audit to gather relevant information to determine the size and scope of the violation;
- Violations must be reported to each organization participating with the HIE in a timely manner; and
- HIEs shall conduct an annual privacy and security audit, and provide the report to the MHCC.

Remedial Actions

HIEs may immediately suspend rights to access the HIE when it is necessary to avoid serious harm to the privacy or security of health information available through the HIE. The suspension can continue until the underlying threat is contained.

- An HIE shall conduct an investigation no later than the next business day if there is a reason to believe that a breach, a non-HIPAA violation has occurred,
- If appropriate an investigation will include an audit,
- Written findings from the investigation will determine if the HIE requires any remedial action to address the non-HOPAA violation of breach,
- The HIE will notify MHCC and the consumer if notification is required under the applicable law, including HIPAA, and
- A consumer may file a written request with MHCC if the person believes that the HIE has acted inappropriately, and MHCC will determine if additional steps must be taken.

Notice of Breach

Both participating organizations and consumers must be notified regarding any violation of PHI through an HIE. An HIE must provide notification to all parties involved no later than 60 days from the time the breach or violation. The notification must include:

- A description of the breach or non-HIPAA violation;
- Information about the patient's right to notify credit reporting agencies of the potential for identity theft or medical identity theft;
- Contact information for the HIE;
- Contact information for at least one credit reporting agency;
- Information concerning the patient's right to opt out of the HIE; and
- Contact information for the Office of the Attorney General Consumer Protection Division and the U.S. Department of Health and Human Services, Office of Civil Rights.

Registration and Enforcement

HIEs must register and annually renew registration with MHCC to operate in the State, which includes providing documentation demonstrating its technical capabilities, and financial viability. There is no fee to register as an HIE. Materials and instructions concerning registration can be found here:

http://mhcc.dhmh.maryland.gov/hit/hie/Pages/hie_registration.aspx.

[4] Sensitive health information is a subset of PHI that includes information with specific legal protections including information protected by current law, such as substance abuse treatment.