# Modernizing Maryland’s Health Information Exchange (HIE) Privacy And Security Regulations

**HIE POLICY BOARD MEETING**

SEPTEMBER 30, 2021

# Background

- December 2019 - MHCC released a Request for Proposals to identify a contractor to propose changes for modernizing COMAR 10.25.18, *Health Information Exchanges: Privacy and Security of Protected Health Information* (regulations)
    - The regulations were adopted in March 2014 and expand upon privacy and security protections established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009
- July 22, 2020 - The Board of Public Works approved MHCC's recommendation to select Post & Schell, P.C. to review the regulations in context of evolving national electronic health information policies

# Key Enhancements

Align with final regulations issued by the Office of the National Coordinator for Health Information Technology on May 1, 2020, to implement certain provisions of the 21st Century Cures Act

- Advance interoperability
- Support the access, exchange and use of electronic health information
- Make patients’ health information more electronically accessible

# Interoperability

- Allows HIEs to share and access health information across disparate systems and increase transparency with consumers

# General Interoperability Provisions

- Reference to the 21st Century Cures Act (which includes interoperability provisions) as applicable law – Section .01D(8)

- Definition of Interoperability – Section .02B(38)

- Definition of 21st Century Cures Act – Section .02B(70)

# Information Blocking

- A practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information

# Preventing Restrictions

- Definition of Information Blocking – Section .02B(37)
- Incorporation of information blocking prohibition and penalties for engaging in information blocking – Section .03D(6)

# Application Programming Interfaces (API)

- Enable different computers, software programs, and applications to easily communicate with one other

# Use of APIs

- Definition of API – Section .02B(2)
- Reference to the right to use a secure third-party smart phone application – Section .03A(5)
- Integration of APIs as a form of communication with consumers – Sections .03H(1)(e) and .03H(5)(b)(v)
- Requirement to implement standardized APIs – Section .05D

# Consumer Access

- Supports the availability of patient health data that can support a patient's control of their health care and medical record

# Removing Barriers & Ease of Access

- Accommodations for translation services and services for hearing or visual impairments – Sections .03B(1)(b)(vii) and (viii) and .03C

- Clarification that any notice or other document required to be in writing may also be provided by electronic means – Section .02B(43)(b)(iv)

- Recognition of a reading comprehension level for all educational materials – Sections .03B(2)(d) and .03H(2)(c)(i)

- Accessibility of notification to a health care consumer – Section .08D(3)

# Information Maintenance & Transparency

- Immediate updates in PHI and access changes across accessible platforms – Sections .03J and .05(F)(1)(c) and (d)
- System administrator data monitoring to ensure information is available immediately to consumers – Section .05H(6)
- Consumer access via expanded platforms to retrieve PHI – Section .03D(2)
- Educational materials for sensitive health information – Section .04A(4)(e)
- Disclosure of PHI for commercial purpose – Section .05(C)

# Privacy & Security

- Protections for electronic health information, expanding upon minimum safeguards established by HIPAA/HITECH and considering existing technology capability

# Patient Privacy, Data Security, Appropriate Authorization, and Access

- Cybersecurity – Sections .03E(1) and (3)(d)
- Updated reference to NIST requirements to allow for use of the most current guidance – Sections .05F(3) and .12A(2)
- Random audits of security measures – Sections .06A(4) and (8)(b)
- Annual compliance audit requirement – Sections .06D and G
- Third party system protocols for improper access – Section .05G(3)(d)
- Auditing policies and procedures for annual privacy and security audit – Section .06C(2)

# Discussion