

IAC BULLETIN

Updates from the MDH Office of Internal Controls and Audit Compliance



HIPAA MATTERS

What is HIPAA?

HIPAA—the Health Insurance Portability and Accountability Act—safeguards the privacy and security of health information that can be used to identify individuals, also known as protected health information (PHI). HIPAA applies to health care providers, health care payers and health care clearinghouses. MDH has elected status as a “Hybrid Entity” because some of its components, such as State Hospitals and Local Health Departments, if they were separate entities, would qualify as providers or payers, while other components, such as Boards and Commissions, would not. When MDH is acting as a provider or a payer (MDH does not have any components that qualify as a clearinghouse), HIPAA applies to our actions and imposes a duty on MDH staff to protect the privacy and security of PHI.



MDH privacy matters are handled through the Privacy Officer within IAC's Compliance Division. The Privacy Officer is responsible for implementing HIPAA and privacy training for MDH staff, investigating potential violations of HIPAA to determine whether a breach has occurred, and advising MDH components on how HIPAA applies to their programs.

For questions about HIPAA, please contact Privacy Officer Lauren Boyce, Lauren.Boyce1@maryland.gov.

The Privacy Rule

HIPAA requires MDH not to disclose PHI except in well-defined, limited circumstances. Disclosure of PHI is permitted when an individual authorizes the disclosure of their own PHI. Other HIPAA permitted disclosures include when the disclosure is made to another provider for patient treatment purposes or when a claim is made to an insurance provider. Sometimes, PHI must be disclosed because it is required by law or because it is the subject of a court order or subpoena. The Privacy Rule also requires that MDH keep any paper records private to avoid unauthorized disclosure. This usually means that paper records should be kept in a secure location such as a locked cabinet when not in use.

For a full explanation of HIPAA-authorized disclosures visit the U.S. Department of Health and Human Services (HHS) online: www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

The Security Rule

The HIPAA Security Rule requires Covered Entities to keep PHI secure. This means that electronic PHI (ePHI) should be stored only on encrypted, password protected devices. Exchange of ePHI should only occur over networks with appropriate security safeguards (encryption, etc.) in place. If ePHI is contained in an email, you must use encryption on the email (Virtu) if you are sending the email.



Report Privacy and HIPAA Violations

The IAC operates a hotline to receive allegations of privacy and HIPAA violations that occur at MDH facilities and components.

Members of the public who believe their rights under HIPAA were violated by an MDH employee or vendor can make a report online.

Visit the IAC website at <https://health.maryland.gov/IAC> and click on "[Report Privacy/HIPAA violations.](#)"



<https://health.maryland.gov/IAC>
MDH.IAC@maryland.gov | 410-767-5314