

# HIPAA, A-Z & Management of Medical Information for Local Governments

2017 Municipal HR & Management Conference

Norman Hanson & DeTroy, LLC  
Robert W. Bower, Jr., Esq.  
Katlyn M. Davidson, Esq.

---

---

---

---

---

---

---

---

## Medical Information Laws to Consider

- HIPAA
- State counterpart to HIPAA
- Freedom of Information Act
- Personnel File Laws
- Americans with Disabilities Act
- Family & Medical Leave Act
- Maine Human Rights Act
- Genetic Information Privacy Act

---

---

---

---

---

---

---

---

## HIPAA

- Health Insurance Portability and Accountability Act of 1996
  - > 42 U.S.C. § 1320d, *et seq.*
- Purpose:
  - > To protect the privacy and security of patient health information and to promote uniformity and confidentiality in the use and transmission of protected health information
- Protected health information ("PHI"): Relates to a medical condition, treatment or payment for health care in any format (oral, written, or electronic)

---

---

---

---

---

---

---

---

## HIPAA - Who does it apply to?

- > Covered entities: Every covered entity is obligated to comply with the Privacy and Security Rules
  
- > Categories of "covered entities":
  - Healthcare providers
  - Health plans
  - Healthcare clearinghouses
  
- > Business Associates

---

---

---

---

---

---

---

---

## HIPAA - Who does it apply to?

- Healthcare providers: Covered by HIPAA if the healthcare provider transmits any health information in electronic form in connection with a healthcare "transaction"
- Transaction: the transmission of information between two parties to carry out financial or administrative activities related to health care, including but not limited to:
  - Health care claims or equivalent encounter information
  - Health care payment and remittance advice
  - Coordination of benefits
  - Health care claim status
  - Enrollment, disenrollment or eligibility in a health plan
  - Health plan premium payments
  - Referral certification and authorization
  - First Report of Injury
  - Health claims attachments

---

---

---

---

---

---

---

---

## HIPAA - Who does it apply to?

- > Business Associates of a covered entity:
  - Businesses to which a covered entity discloses protected health information so that the business can perform or assist in certain services on behalf of a covered entity
  - Functions such as claims processing and administration, billing or benefit management, data analysis, data storage, etc. or provides legal, actuarial, accounting, consulting, administrative or financial services.

---

---

---

---

---

---

---

---

## Does HIPAA apply to municipalities and counties?

- > Yes, IF: The municipality or county is a covered entity or business associate.
- > Municipalities/counties are often covered due to serving as a healthcare provider or the sponsor of a health plan
  - Common examples of qualifying healthcare providers: Hospitals, public health clinics, correctional facilities with health clinics, ambulance/emergency medical services
  - Health plan: A municipality sponsors a health plan or if it offers its employees medical covered or medical expense reimbursement
    - Sponsorship not dependent on funding
    - Includes dental, vision and prescription drug coverage, employee assistant plans (EAPs), and medical expense reimbursement arrangements

---

---

---

---

---

---

---

---

## HIPAA – Hybrid Entity

- Hybrid entity defined:
  - > (1) A single legal entity that has both covered and non-covered component, and
  - > (2) Designates itself a hybrid entity by identifying covered health care components
- Advantage: Limits liability exposure for HIPAA violations to only the covered functions
- Municipality must designate itself as a hybrid entity; otherwise, all PHI maintained by the entity is subject to HIPAA regulations

---

---

---

---

---

---

---

---

## HIPAA – Hybrid Entity

- Designation: No requirement to file designation papers with any governing body; Published declarations are common
- Categories that must be treated as covered components:
  - > Any component that would qualify as a covered entity if it was a separate legal entity
  - > Any component that would be considered a business associate
- Requirements:
  - > Implement firewalls to prevent inappropriate use and disclosure between covered and non-covered components
  - > Staff within the covered component required to comply with all privacy and security regulations

---

---

---

---

---

---

---

---

## HIPAA – Privacy & Security Requirements

- Authorizations from individual required for any use or disclosure of PHI that is not for treatment, payment or healthcare operations or otherwise permitted or required by law
- Examples: Disclosure to life insurer, disclosure to employer for pre-employment physicals
- Authorizations must:
  - > Be in plain language
  - > Include specific information regarding what to be disclosed or used
  - > Person disclosing and receiving the information
  - > Expiration
  - > Right to revoke

---

---

---

---

---

---

---

---

## HIPAA – Privacy & Security Requirements

- Must have written privacy policies and procedures
- Must develop and implement policies re: access restrictions for the workforce of covered entities
- Must establish and implement policies/procedures for routine recurring disclosures or requests for disclosures

---

---

---

---

---

---

---

---

## HIPAA – Privacy & Security Requirements

- Personnel: Must designate a privacy official and contact person or office for complaints
- Training: All workforce members must be trained on privacy policies and procedures
- Data safeguards: Must take reasonable safeguards to prevent intentional or unintentional use or disclosure of PHI
  - > Shredding documents
  - > Password protection
  - > Records kept locked

---

---

---

---

---

---

---

---

## HIPAA – Privacy & Security Requirements

- Privacy Practices Notice
  - > Must provide a notice of the covered entity's privacy practice
  - > Must describe the way in which the covered entity may use and disclose PHI
  - > Must state duties to protect privacy
  - > Must describe individual's rights, including right to complain to HHS and to the entity
  - > Must include a point of contact for further information or for complaint

---

---

---

---

---

---

---

---

## HIPAA – Privacy & Security Requirements

- Privacy Practices Notice – Distribution
  - > Health care provider with direct treatment relationship:
    - Must deliver notice no later than first service encounter
    - Must post notice at each service delivery site
    - Must make good faith effort to obtain written confirmation from patients of receipt of notice
  - > Emergency situations: Furnish notice as soon as practicable
  - > Health plan: Notice to each new enrollee at time of enrollment and reminders to every enrollee at least once every 3 years

---

---

---

---

---

---

---

---

## HIPAA – Obligations re: Breach

- Duty to identify and respond to any "security incident" including an impermissible disclosure known or suspected
- Duty to notify in case of breach of unsecured PHI
- Duty to document incident and retain for 6 years
- Duty to apply sanctions against employee
- Duty to mitigate if possible

---

---

---

---

---

---

---

---

## HIPAA – Exceptions to Privacy Rules

- ◉ Covered entities may use or disclose PHI without the authorization of the individual when the use or disclosure is:
  - > For treatment, payment or health care operations of a covered entity
    - Treatment includes coordination or management of health care and related services by one or more health care providers, consultation between providers, and referral of patients for treatment
  - > Required by law
  - > For certain public health activities/reporting authorized by law (e.g., communicable diseases, births, deaths, child abuse or neglect)
  - > For judicial and administrative proceedings in response to an order or subpoena
  - > For law enforcement purposes (e.g., mandatory reporting)
  - > Reporting crime in emergencies
  - > To avert a serious threat to health or safety of a person or the public
  - > Specialized government functions, e.g., correctional institutions and custody in law enforcement
  - > Workers' compensation
- ◉ Note: these exceptions are not an exhaustive list and only to the extent specifically permitted or required by law
- ◉ Limit disclosure to the "minimum necessary" (except for purposes of treatment)

---

---

---

---

---

---

---

---

---

---

## HIPAA – Exception to PHI

- ◉ Excluded from the definition of protected health information is individually identifiable health information in employment records held by a covered entity in its role as an employer. 45 C.F.R. § 160.103

---

---

---

---

---

---

---

---

---

---

## Federal HIPAA vs. State Law re: medical confidentiality

- ◉ HIPAA preempts contrary state law unless:
  - > State law provides greater privacy protections and greater individual rights
- ◉ Maine analog to HIPAA – 22 M.R.S.A. § 1711-C
  - > Two areas of Maine law may be considered more protective:
    - Presumes written authorization for release
    - Imposes a 30 month time limit for written authorizations

---

---

---

---

---

---

---

---

---

---

## Office for Civil Rights (“OCR”)

- Division of U.S. Department of Health & Human Services
- Tasked with enforcing HIPAA and investigating health information privacy complaints
  - > State Attorney General also authorized to bring civil actions
- Also conducts compliance reviews of covered entities
- [www.hhs.gov/hipaa](http://www.hhs.gov/hipaa)

---

---

---

---

---

---

---

---

## Office for Civil Rights (“OCR”) Investigation Process

- Anyone can file a complaint; must be filed within 180 days of when the complainant knew that the alleged violation occurred. OCR can extend the 180 day period if “good cause” shown
- If OCR accepts complaint, covered entity will be notified
  - > Both sides asked to present information about alleged violation; OCR may ask for specific information
  - > Covered entities are required by law to cooperate with complaint investigations

---

---

---

---

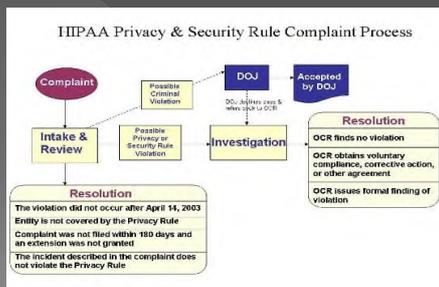
---

---

---

---

## Office for Civil Rights (“OCR”) Investigation Process



---

---

---

---

---

---

---

---

## Office for Civil Rights (“OCR”) Investigation Process

- If satisfactory action not taken to resolve the matter, OCR can impose civil money penalties
  - > Covered entity may request a hearing before an HHS ALJ to decide if penalties are supported by the evidence

---

---

---

---

---

---

---

---

## Mental Health, Homicide, Suicide and Aggravated Assault Review Board

- This Board reviews homicides, suicides and aggravated assaults involving persons with severe and persistent mental illness. It makes recommendations to state and local agencies of methods for preventing these events, including modifications of laws, rules, policies and procedures.
- The Board is authorized to collect data related to these issues. Any person in possession of such data must provide the information and records to the board as soon as practicable.
- Those providing such data are immune from criminal and civil liability for the disclosure.
- 34-B M.R.S.A. § 1931

---

---

---

---

---

---

---

---

## Other State Laws Regarding Protected Health Information

---

---

---

---

---

---

---

---

## Local Health Officers

- Every municipality in the State shall employ a local health officer who is appointed by the municipal officers of that municipality.
- Local Health Officers must complete at least one six-hour training every three years to meet the required Local Health Officer qualifications.
- Records in their possession subject to FOAA.
- 22 M.R.S.A. § 451 *et seq*

---

---

---

---

---

---

---

---

## Freedom of Access Act (FOAA)

- Records of public actions are open to review by the public.
- Law to be liberally construed in favor of access, and interpreted *de novo* by the Supreme Judicial Court.
- Entities covered by FOAA: Any board, commission, agency or authority of any county, municipality, school district or any other political or administrative subdivision.
- 1 M.R.S.A. §401 *et seq*

---

---

---

---

---

---

---

---

## Public Records Under FOAA

- Written, graphic, electronic
- In possession of official
- Received or prepared for use in connection with transaction of public or government business, or contains such information
- Section 402(3)

---

---

---

---

---

---

---

---

## Exceptions to Public Records

- Records designated as confidential elsewhere in statutes.
- Records protected by privilege against discovery or use in civil or criminal trial.
- Medical records and reports of municipal rescue and emergency medical services, except that such records must be made available to law enforcement officers investigating criminal conduct.
- Juvenile records of municipal fire departments regarding the investigation and family background of a juvenile fire setter.
- Personally identifying information concerning minors maintained by municipalities for recreation and nonmandatory educational services and programs IF ordinance adopted.
- Social Security numbers.
- Personal contact information for public employees [not including elected officials].
- Section 402(3)

---

---

---

---

---

---

---

---

---

---

## Information Deemed Not a Public Record

- Medical information possessed by MEPERS
  - › Except that public employers can review medical information possessed by MEPERS for any purposes related to any claim for workers' compensation or any other benefit. The employee must be advised in writing by MEPERS that the employer has requested review of his or her medical records.
  - › 5 M.R.S.A. § 17057
- Medical information of any kind from personnel records for municipal and county employees
  - › 30-A M.R.S.A. § 2702 (Municipal)
  - › 30-A M.R.S.A. § 503 (County)
- Records concerning quality assurance activities of an emergency medical services quality assurance committee are confidential and may not be disclosed. Such records can be shared with a licensee as part of education or correction.
  - › 32 M.R.S.A. § 81 *et seq*

---

---

---

---

---

---

---

---

---

---

## Tampering with public records

- Destroying, altering, concealing public records is considered a Class D crime
- 17 M.R.S.A. § 456

---

---

---

---

---

---

---

---

---

---

## Employee Right to Review Personnel File

- An employer shall provide the employee's personnel file to the employee for review and copying
- Requires a written request from the employee
- Employer has 10 days to comply
- Personnel file includes "nonprivileged medical records and nurses' station notes."
  - > "Nonprivileged" means materials that not been found to be protected from discovery or disclosure in civil litigation
- Maximum forfeiture of \$500 plus attorney fees
- 26 M.R.S.A. §631

---

---

---

---

---

---

---

---

## Americans with Disabilities Act

- Prohibits discrimination against a qualified individual with a disability because of the disability in regards to application for employment or employment

---

---

---

---

---

---

---

---

## Americans with Disabilities Act

- Disability inquiries and medical exams:  
An employer may make disability related inquiries and request medical exams of employees only if they are "job-related and consistent with business necessity."
- Applies to all employees; not just employees with disabilities

---

---

---

---

---

---

---

---

## Americans with Disabilities Act

- ◉ An inquiry or exam is job related and consistent with business necessity when:
  - > Employer has reasonable belief based on objective evidence:
    - (1) an employee's ability to perform essential job functions will be impaired by a medical condition; or
    - (2) an employee will pose a direct threat due to a medical condition

---

---

---

---

---

---

---

---

## Americans with Disabilities Act

- ◉ Direct threat: significant risk of substantial harm to the health or safety of the individual or others that cannot be eliminated or reduced by reasonable accommodation

---

---

---

---

---

---

---

---

## Americans with Disabilities Act

- ◉ Limitations on employer ability to share information
  - > Supervisors & managers: can know necessary restrictions and necessary accommodations only
  - > First Aid and Safety Personnel: may be informed when appropriate if disability might require emergency treatment
- ◉ Confidentiality of medical information
  - > Separate forms
  - > Separate from personnel file

---

---

---

---

---

---

---

---

## Maine Human Rights Act

- Unlawful for an employer to elicit information pertaining to race, color, sex, sexual orientation, physical or mental disability, religion, age, etc.
- Unlawful to make or keep a record of race, color, sex, sexual orientation, physical or mental disability . . .
  - › Exception for records of disability

---

---

---

---

---

---

---

---

## Maine Human Rights Act

- Permissible exams and inquiries:
  - › If job related and consistent with business necessity
  - › Employer can make inquiries into employee's ability to perform job
- Records of disability
  - › Confidential
  - › Separate forms
  - › Separate file

---

---

---

---

---

---

---

---

## Maine Human Rights Act

- Restrictions on who can know:
  - › Supervisors & Managers – Limited to necessary restrictions on work duties & necessary accommodations

---

---

---

---

---

---

---

---

## Family & Medical Leave Act

- Eligible employees have the right to unpaid protected leave for specified family and medical reasons
- Certification of a serious health condition
  - > Prescribed Forms
  - > Limitations on what information an employer can obtain
  - > Clarification and authentication can only be requested by a health care provider, H.R. professional, leave administrator or management official
  - > "Under no circumstances" may a supervisor contact the employee's health care provider; 29 C.F.R. 825.307(a)
- No HIPAA exemption

---

---

---

---

---

---

---

---

## Family & Medical Leave Act

- Recordkeeping requirements:
  - > Must be maintained as confidential
  - > In separate files from the usual personnel file

---

---

---

---

---

---

---

---

## Genetic Information Nondiscrimination Act

- Prohibits employers from using genetic information to make employment decisions
- Prohibits employers from intentionally acquiring genetic information
- Must keep genetic information confidential
- Genetic information = genetic tests of individual & family members and family medical history

---

---

---

---

---

---

---

---