Health Information Privacy Laws

2018 HIPAA & FERPA Update

Maine AAP Conference

April 14, 2018

Key Question

What *legal authority* do I/we have for disclosure of health information to a third party?

Confidentiality Laws

- **Maine Statutory Law**: 22 M.R.S.A. §1711-C
  - Confidentiality of Health Care Information
- **HIPAA**: 42 U.S.Code § 300gg and 29 U.S.Code § 1181 *et seq.* and 42 U.S.Code § 1320d *et seq.*
  - Health Information Portability and Accountability Act
- **FERPA**: 20 U.S.Code § 1232g
  - Family Educational Rights & Privacy Act

Maine Confidentiality Law

- 22 M.R.S.A. §1711-C:
  - Makes health care information confidential and prohibits unauthorized disclosure
  - Requires policies, standards & procedures to protect the confidentiality, security & integrity of health care information
  - Requires an authorization from patient for releases of information (with exceptions in law)
  - Imposes penalties for violations

Preemption of State Law

- Federal law preempts contrary state law unless a state privacy law is more "stringent" than the standard in the rule or a specific exception applies

What is HIPAA?

The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct

- Establishes rules for privacy, security, and electronic transmission of data.
- Sets boundaries on the way providers use and release protected health information (PHI);
- Establishes safeguards that we must achieve to protect the privacy of PHI;
- Provides for adverse consequences including fines and jail sentences for failure to comply.

HIPAA

What is **P**rotected **H**ealth **I**nformation (PHI)?

- All individually-identifiable health information transmitted or maintained in any medium
  - Health information: information related to past, present or future health condition of, treatment of, or payment for treatment of, an individual

Some "Health" Records are Not PHI under HIPAA

- School records are education records under FERPA, not health records
- Schools not considered "covered entities" under HIPAA ***unless*** they employ a health care provider that conducts one or more covered transactions (i.e., billing a health plan) electronically

HIPAA

Uses & Disclosures of PHI

- Required disclosures
- Permitted disclosures
- Disclosures for which there is an opportunity to agree or object
- Other permitted disclosures: authorized by other laws, no consent or opportunity required

HIPAA Required Disclosures

- To the individual
  - Patient has broad right of access to his/her health care information
  - Provide access to "designated record set" (including medical & billing records)
  - Practice may require patient to pay "reasonable costs"
  - If EHR, **must be able to request in electronic form** (and only charge for *actual* labor & supply costs)

Limits on HIPAA or Maine Right to Access Records

- Maine law allows exclusion of "personal notes" not directly related to the patient's past or future treatment
- Maine law allows for release of information to "authorized representative" instead of patient, if release to the patient would be "detrimental to the health of the patient"
- HIPAA requires detailed description of how an individual can request a review of denial

HIPAA Permitted Disclosures

- For **Treatment**, **Payment** or Health Care **Operations**
  - Provision, coordination or management of health care & related services
  - Activities to obtain reimbursement
  - QA & QI activities
  - But, special considerations given to records containing **mental health, alcohol** and **drug abuse** treatment and **HIV** test results

HIPAA Permitted Disclosures

- Pursuant to a valid authorization
  - Applies to uses & disclosures NOT related to treatment, payment or health care operations
  - **Required** for marketing purposes
    - But, marketing is not disease management, wellness programs, prescription refill reminders, appointment notices if practice receives *no compensation* (see new HIPAA rule)

13

No Consent, Authorization or Opportunity

- Those required by law (i.e. court order; Medicare condition of participation)
- Public health activities (i.e. gun shot reporting, notifiable disease reporting)
- Victims of abuse, neglect, or domestic violence
- Health oversight activities (i.e. auditing or licensing matters)
- Judicial & administrative proceedings
- Information about decedents: coroners, medical examiners, & funeral directors
  - ***To family members of decedents*** who were involved in care/payment
  - 50 years after death

15

Opportunity to Agree or Object

- No written consent or authorization required
  - Facility directories (e.g. listing name, location, condition)
  - Persons involved in the individual's care (e.g. family member, friend)
  - Disaster relief

14

No Consent, Authorization or Opportunity

- **Law enforcement** purposes
  - Note: Maine law allows reporting to law enforcement if prescriber "knows or has reasonable cause to believe that a person is committing or has committed deception (17-A MRSA sec. 1108) or a crime on the premises or against provider
- Organ, eye, or tissue **donation**
- **Research** purposes (within constraints)
- To avert a serious **threat** to health or safety
- For specialized **government** functions: military, public benefits, workers comp

16

Minimum Necessary

- Practices should disclose or use only the minimum necessary amount of PHI in order to be responsive to the request
- Minimum Necessary does NOT apply to:
  - Disclosures for treatment
  - Disclosures to the individual requesting their own record
  - Disclosures pursuant to a valid authorization
  - Disclosures required by law or to HHS

17

Incidental Uses & Disclosures

- Waiting room sign-in sheets
- Patient charts at bedside
- Physician conversations with patients in semi-private room
- Physicians conferring at nurse's stations

18

HIPAA Patient Rights

- Notice of privacy practices
- Right to request restriction of use or disclosure
- Access
- Amendment
- Accounting of disclosures

19

Amendment

- Patient has right to request amendment of PHI
- Entity must respond within 60 days
  - **Grant** request & update records to reflect
  - **Deny** request & provide written explanation
  - **Extend time** for no more than 30 days
  - If request denied, patient has right to include letter of disagreement in record

20

HIPAA Business Associates

- PHI may be disclosed to a Business Associate if the Covered Entity has executed a Business Associate Agreement
- HIPAA requirements extend directly to the BA
  - E.g., must have all policies, procedures & safeguards in place
  - Now subject to HIPAA civil & criminal penalties

21

Breach Notification

- OLD analysis (until 9/23/13):
  - Only report a breach of unsecured PHI if there was significant risk of financial, reputational or other harm
- NEW analysis (after 9/23/13)
  - Presume breach must be reported unless a risk analysis shows a low probability that the information was compromised

22

What is FERPA?

The **F**ederal **E**ducational **R**ights & **P**rivacy **A**ct

- Applies to public elementary, secondary and post-secondary schools
- Gives parents certain rights:
  - Access to and right to amend children's education records
  - Some control over disclosure of personally identifiable information

23

FERPA Records

- Records directly related to student, maintained by school or its agent
  - Kept in ANY medium (including Email!)
  - "PII": **P**ersonally **I**dentifiable **I**nformation
- Include grades, transcripts, class lists, course schedules, **health records**
- No particular types of information are required by FERPA to be kept

24

FERPA Excluded Records

Not considered education records if:

- Kept in sole possession of maker, not accessible or revealed to others
  - If revealed, they become educational records
- Examples: "personal" notes of meetings, telephone calls
- Law enforcement records

25

FERPA Disclosures

- Must keep specific, detailed records of all requests for and disclosures of PII
- Right to inspect before disclosure
- Exceptions:
  - Parent (and student, if eligible)
  - Person with parent's written **consent**
  - School officials as defined in FERPA
    - "Legitimate educational interest"
  - Transfer to new school

26

FERPA Exceptions

May disclose records without consent if:

- Health or safety **emergency** (limited)
  - Actual, impending or imminent
  - NOT for exercises!
- Articulable and significant **threat**
- Subpoenas and **court** orders, or allowed by state law to juvenile justice
  - Requires reasonable effort to notify parent

27

FERPA Exceptions

Several other limited exceptions, such as for audits, accreditation, studies, etc.

28

Other FERPA Issues

- Directory information may be disclosed
- Notification of rights required
- Staff training required
- Breach notification not required
- Waiver of some rights allowed (e.g., right to see recommendation letters)

29

Questions?

Maine Medical Association
30 Association Drive, P.O. Box 190
Manchester, Maine 04351
207-622-3374
207-622-3332 Fax
gsmith@mainemed.com
amaclean@mainemed.com
pmichaud@mainemed.com

30