

Health Information Privacy Laws

2018 HIPAA & FERPA Update ***with special emphasis on Minors' Rights***

Greater Portland Health
July 11, 2018

Gordon H. Smith, Esq.
Maine Medical Association

Disclosure

There are no significant or relevant financial relationships to disclose.

Recent Developments

Advocate Health System \$5.5 million for three data breaches that occurred in 2013. In total, the three incidents compromised the protected health information of 4 million individuals. Incidents involved laptop theft and hacking.

CardioNet (Cardiac monitoring company)

\$2.1 million for failure to have security management process, policies & procedures for handling computer hardware & electronic media

Presence Health Network

\$475,000 for untimely reporting of breach to individual, news outlets & HHS

Center for Children's Digestive Health

\$31,000 for failure to have Business Associate Agreement with records storage company

OCR Increasing Scrutiny

HHS' Office for Civil Rights is becoming more aggressive in enforcing HIPAA:

- In the first seven months of 2016 alone, HHS recorded close to \$15 million in settlement payments
- Investigated and resolved over 25,167 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates
- As of May 31, 2017, settled 52 cases resulting in a total dollar amount of \$72,929,182.00
- Most frequently investigated complaints against (in order): private practices, general hospitals, outpatient facilities, pharmacies, health

News Flash!

Physicians' health information privacy obligation is not new!

HIPAA introduced new terms & give guidance, but do not substantially change physicians' obligations

Key question for the health care practitioner or practice: what *legal authority* do I/we have for disclosure of health information to a third party?

Confidentiality Laws and Rules

- Substance use disorder treatment program records
 - 42 C.F.R. Part 2
- HIPAA Privacy Rule
 - 45 C.F.R. Parts 160 and 164
- Maine health care information confidentiality law
 - 22 M.R.S. § 1711-C
- Records of licensed mental health agencies or facilities
 - *34-B M.R.S. § 1207*
 - *Rights of Recipients of Mental Health Services*
 - *Rights of Recipients of Mental Health Services Who Are Children in Need of Treatment*
- HIV/AIDS diagnosis or treatment information
 - 5 M.R.S. §§ 19201, 19203, 19203-D, and 19205
- Other?

Source: Kozak & Gayer, P.A.

What is HIPAA?

The Health Insurance Portability and Accountability Act

- HIPAA establishes rules for privacy, security, and electronic transmission of data. This training focuses on privacy.
- 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

HITECH

- Found in American Recovery and Reinvestment Act of 2009
- Health Information Technology for Economic and Clinical Health Act
- Modifies certain aspects of HIPAA
- Most known for “breach reporting” requirement

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
- 2 aspects of Maine law may be more “stringent”
 - Presumes written authorization for release
 - 30-month limit for written authorizations for release

What is Protected Health Information?

- 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 Records are Not PHI

- School records
- Prison records
- Employee records

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**

Required Disclosures

- To the individual
 - Current presumption: patient has broad right of access to his/her health care information
 - Provide access to “designated record set” (including medical & billing records) or, if patient consents, a summary of the records
 - Practice may require patient put request in writing
 - Practice may require patient to pay “reasonable costs” – \$5 for first page and \$.45 for each additional page
 - If EHR, **must be able to request in electronic form** (and only charge for *actual* labor & supply costs)

Permitted Disclosures

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

Permitted Disclosures

- Pursuant to a valid authorization
 - Applies to uses & disclosures NOT related to treatment, payment or health care operations
 - But, is required for treatment by a mental health professional, drug/alcohol abuse treatment & HIV test results
 - 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)
 - Many exceptions to when required (see below)

42 CFR Part 2 Requirements

- Policies:
 - Confidentiality
 - Security of Records
- Notice: Prohibition on Re-Disclosure of Information
- Summary of Confidentiality Laws and Rules
- Disclosure Log
 - For disclosures *outside* scope of “Universal Release”
- Training

Access to Mental Health Records

Recent law improving access to mental health records

- Prior Law: requires patient authorization for disclosure of health info outside of the office/facility if it reflects mental health services provided by clinical nurse specialist, psychologist, social worker, LCPC or psychiatrist.
- New Law: allows disclosure without authorization to a health care practitioner, facility or payor for purposes of care management or coordination of care. Disclosure of psychotherapy notes remains governed by HIPAA. Must make a reasonable effort to notify the individual of the disclosure.

No Consent or Authorization Required

- 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

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

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

Incidental Uses & Disclosures

- Incidental Uses & Disclosures are permitted if:
 - They cannot be reasonably prevented;
 - Are limited in nature;
 - Are a by-product of otherwise permitted use;
and
 - The Covered Entity has established “reasonable safeguards” to ensure only necessary information is disclosed

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

Patient Rights

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

Notice of Privacy Practices

- Note: HIPAA rules require practices to update their notice
 - MMA HIPAA site for model forms
<http://www.mainemed.com/education-info-cme/hipaa>
 - Updated notice will have to be posted & made available to patients
- The uses & disclosures of PHI that may be made by the covered entity
- The individual's rights & the covered entity's duties re: PHI
- Complaint procedures
- Contact information
- Effective date

Request for Limitations

- Individuals may request specific restrictions on use and disclosure
- *Physicians now required to abide by patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction*
- If for treatment, covered entity can deny

Access

- Patient right to request to inspect records
- Addressed above under Maine law

Administrative Requirements

- Designated privacy official & complaint contact person
- Staff training
- Administrative, technical, & physical safeguards
- Complaint procedure, including documentation of complaints & their resolution
- Must maintain policies & procedures in written or electronic form for 6 years

Compliance & Enforcement

- Now under HITECH:
- State Attorneys General authorized to bring civil actions
- DHHS accorded authority to prosecute criminal actions
- Security audits by OCR

Potential Sanctions

- *Civil*: \$100-\$50,000 per violation, depending on “culpability” (with caps per year)
- *Criminal*:
 - From \$50,000 & 1 year imprisonment (“wrongful disclosure”) to
 - \$250,000 & 10 years imprisonment (for “commercial gain”)

Breach Notification

- Factors that MUST be considered:
 1. The nature & extent of PHI involved
 - E.g. sensitive data such as financial info, SSN, detailed clinical data and/or ability to re-identify more concerning
 2. The unauthorized person who used the PHI/to whom disclosure was made
 - E.g. another HIPAA covered entity less concerning
 3. Whether the PHI was actually acquired or viewed
 4. The extent to which the risk to PHI has been mitigated
 - E.g. can recipient give assurances PHI was destroyed

Breach Notification (cont.)

- If Yes, have 60 days to notify patient unless
 - Unintentional acquisition within same entity, within scope of authority, no further disclosure
 - Fax received by billing not lab
 - Inadvertent disclosure to member of same entity & no further disclosure
 - Email to wrong dept, deleted
 - Good faith belief that PHI cannot be retained
 - Immediately recovered from wrong person

Breach Notification (cont.)

- Notification requirements
 - Brief description of event
 - Date of breach & discovery
 - Description of information disclosed
 - Any steps to take to protect themselves
 - Steps entity is taking to mitigate, prevent
 - Contact information
- Notify HHS
 - Immediately if > 500 individuals; or yearly log
- Document in accounting
- Further requirements if SSN, credit card or other sensitive info disclosed or if >500

Related Medical Record Issues

- Ownership of the medical record
- Retention of medical records
- Disposal of medical records
- Prescription Monitoring Program
- Subpoenas for medical records
- Minors' medical records
 - Retention
 - Divorced parents

Aspects of Minors' Health Care

- Consent to treatment
- Access to & control of PHI & medical records
- Related issues

Consent to Treatment

- AMA Code of Medical Ethics Opinion 8.08, *Informed Consent*
 - “Patient’s right of self-decision[:]” “The physician’s obligation is to present the medical facts accurately to the patient . . . and to make recommendations for management in accordance with good medical practice.”
- Early case law on informed consent
 - Schloendorff v. Society of New York Hospital, 211 N.Y. 125, 105 N.E. 92 (1914): surgery without patient consent = assault
 - Salgo v. Leland Stanford Jr. University Board of Trustees, 317 P.2d 170 (1957): first judicial opinion to use term “informed consent”
- Key elements
 - The nature & purpose of the treatment
 - The risk & consequences involved in the treatment
 - Alternative courses of treatment, including the consequences of no treatment
 - An opportunity for the patient to ask questions

General Rule

- Minor: an individual who has not yet reached 18 years of age
- Practitioners must obtain consent of a parent or guardian for treatment of a minor, although the minor generally is involved in the process
 - Generally accepted that one parent may consent to treatment, but note *Donna L. Andrews v. The Board of Social Worker Licensure*, Cumberland County Superior Court Docket No. AP-05-008, 9/2/05
- Capacity: “Incapacitated person” means one who is “impaired by reason of mental illness, mental deficiency, physical illness or disability, chronic use of drugs, chronic intoxication, or other cause except minority to the extent that he lacks sufficient understanding or capacity to make or communicate responsible decisions concerning his person.” 18-A M.R.S.A. §5-101(1)

Exceptions to the General Rule

- Emergency care. AMA Ethics Opinion 8.08, *Informed consent*; 24 M.R.S.A. sec. 2905, *Informed consent to health care treatment*.
- Minor's status. *Some* minors may consent to *all* health care treatment.
- Sensitive types of treatment. *All* minors may consent to *some* health care treatment.

Minor's Status

- A minor may consent to all types of treatment if he/she meets 1 or more of the following:
 - Independent. Minor has been living separately from parents or guardians for at least 60 days & is independent of parental support.
 - Married. Minor is or was legally married.
 - Military. Minor is or was a member of the Armed Forces of the U.S.
 - Emancipated. Minor has been emancipated by the court pursuant to 15 M.R.S.A. sec. 3506-A (age 16 or older).

22 M.R.S.A. sec. 1503.

Sensitive Types of Treatment

- All minors may give consent to certain sensitive types of treatment where an obligation of parental consent may be an obstacle to treatment and, therefore, may not be in the best interest of the minor.

Sensitive Types of Treatment Include

- Family planning services, including contraception, pregnancy testing, & emergency contraception. 22 M.R.S.A. sec. 1908. (prenatal & OB services?)
- Treatment of venereal disease or drug or alcohol abuse by a physician. 32 M.R.S.A. secs. 2595 & 3292.
- Treatment of drug or alcohol abuse or for emotional or psychological problems. 22 M.R.S.A. sec. 1502.
- Certain services provided by alcohol & drug counselors, social workers, or psychologists. 32 M.R.S.A. secs. 6221, 7004, & 3817.

Sensitive Types of Treatment Include (continued)

- Treatment of venereal disease or drug or alcohol abuse in the hospital setting, but parental consent is required if hospitalization continues for more than 16 hours. 22 M.R.S.A. sec. 1823.
- Collection of sexual assault evidence through a sexual assault forensic examination. 22 M.R.S.A. sec. 1507.
- Consent to give blood by a 17 year-old. 22 M.R.S.A. sec. 1502-A.

Sensitive Types of Treatment: Abortion Services

- A minor may consent to an abortion if she accomplishes *one* of the following:
 - Provides the physician performing the abortion with her informed written consent & the written consent of a parent or another adult family member such as an aunt or grandmother.
 - Provides the physician performing the abortion with her informed written consent & receives abortion counseling from a physician or an approved counselor who may be a psychiatrist, psychologist, social worker, ordained clergy member, PA, NP, guidance counselor, RN, or LPN.
 - Provides the physician performing the abortion with her informed written consent and a court order.

22 M.R.S.A. sec. 1597-A.

Practitioner Retains Discretion to Notify Parents

- Statutory provisions regarding sensitive types of treatment *permit* but *do not require* practitioners to rely on minor's consent.
- Practitioner retains the discretion to notify the parents if he/she believes that failure to do so would “seriously jeopardize the health of the minor or would seriously limit the practitioner’s or provider’s ability to provide treatment.” 22 M.R.S.A. sec. 1505(2).

Immunity for Good Faith Reliance on Minor's Consent

- A practitioner who takes reasonable steps to determine that a minor is entitled to consent to health care treatment is immune from liability for a parent's claim that the practitioner provided care without parental consent.

22 M.R.S.A. sec. 1504.

General Rule

- Parents have the legal authority for control of & access to PHI & medical records of a minor.

Consenting Minor Controls PHI & Medical Records

- However, a minor who consents to health care treatment is entitled to the same confidentiality rights as adults. 22 M.R.S.A. sec. 1505(1).

Relevant Health Information Privacy Laws

- “General” privacy laws
 - HIPAA Privacy Rule, 45 C.F.R. Parts 160 & 164
 - 22 M.R.S.A. §1711-C, Confidentiality of health care information
- Additional privacy laws specifically addressing behavioral health
 - 42 U.S.C. §§290dd-2 & 42 C.F.R. Part 2, Confidentiality of drug & alcohol abuse patient records statute & regulations
 - 34-B M.R.S.A. §1207, Confidentiality of information
 - Bureau of Children with Special Needs Rule Chapter 1, *Rights of Recipients of Mental Health Services who are Children in Need of Treatment*

Financial Responsibility

- In general, a minor who consents to health care treatment is financially responsible to the practitioner for that treatment. 22 M.R.S.A. sec. 1506.
- Risk of breach of confidentiality through EOB of minor covered by parents' health insurance?

Rights of Divorced Parents to Access PHI

- Family law presumption is “*shared* parental rights & responsibilities.”
- Generally, this means that each divorced parent has the right to participate in medical decision-making for the minor child & to access PHI.
- Where the child resides & the parent with whom the practice has the primary relationship has no bearing on access.

Court Order Must Include

- “A statement that each parent must have access to records and information pertaining to a minor child, including, but not limited to, medical, dental and school records and other information on school activities, whether or not the child resides with the parent, unless that access is found not to be in the best interest of the child or that access is found to be sought for the purpose of causing detriment to the other parent. If that access is not ordered, the court shall state in the order its reasons for denying that access.”

19-A M.R.S.A. sec. 1653(2)(D)(4).

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