Health Information Privacy Refresher Training
Topics for Today

• State health information privacy law
• Federal health information privacy law
• Recent changes in HIPAA privacy & security rules
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?
Maine P.L. 1999, Chapter 512

22 M.R.S.A. §1711-C
Confidentiality of Health Care Information
Maine Confidentiality Law

- 22 M.R.S.A. §1711-C already:
  - 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
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

Maine Medical Association 30 Association Drive, PO Box 190 Manchester, ME 04351  ph 207.622.3374 fax 207.622.3332  www.mainemed.com
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 to put request in writing
  - Practice may require patient to pay “reasonable costs” - now limited to $10 for first page and $.35 for each additional page copied
  - If EHR, must be able to request in electronic form (and only charge for labor)
Limits on 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” if release to the patient would be “detrimental to the health of the patient.”
- HIPAA requires you describe in detail how an individual can request a review of the denial.
Required Disclosures

- To the Department of Health and Human Services for purposes of determining compliance with the Privacy Rule
Permitted Disclosures

- For Treatment, Payment or Health Care Operations
  - Provision, coordination or management of health care & related services
  - Activities to obtain reimbursement for the provision of care
  - QA & QI activities
Consent

- Consent not required for TPO purposes
- Bush Administration emphasized use of Notice of Privacy Practices instead
- Physician practice may implement consent process & may condition treatment on consent
• Consent form may be combined with other forms but NOT with the Notice of Privacy Practices
• Consent may be revoked at any time except to the extent it has been relied on
• Signed consent must be retained
Consent Form Standards

- Plain language
- Inform of uses for TPO
- Refer to Notice of Privacy Practices
- Advise that individual can request restrictions but covered entity need not agree
- Advise of right to revoke, except to extend relied on
- Signed & dated
Permitted Disclosures

• Pursuant to a valid authorization
  - Applies to uses & disclosures NOT related to treatment, payment or health care operations
    • But, is required for psychotherapy notes
  - Required for marketing purposes
    • But, marketing is not disease management, wellness programs, prescription refill reminders, appointment notices
  - Many exceptions to when required (see below)
Authorization Form Standards

- Plain language
- Meaningfully describe the information that will be used or disclosed
- Identify the person or class or persons authorized to make the requested use or disclosure
- Identify the person or class or persons who may use the information or to whom it may be disclosed
More Authorization Form Standards

- Expiration date
  - Note: Maine law applies a 30-month limit for written releases
- Description of revocation requirements
- Warn about potential for re-disclosure & loss of privacy protection
- Signed & dated
Authorization Standards

- **May not** condition treatment, payment, or eligibility for benefits on the individual’s giving an authorization
- Retain authorizations for 6 years from date of creation or date last in effect whichever is later
- Provide a copy to the individual
Opportunity to Agree or Object

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

• Information about decedents: coroners, medical examiners, & funeral directors

• 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 do their jobs

• Minimum Necessary does NOT apply to:
  - Disclosures for TPO
  - Disclosures to the individual requesting
  - Disclosures pursuant to valid HIPAA 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

- 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
“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.”
Providers with a “direct treatment relationship” must make good faith effort to obtain or document reasons for failure.

- Must be in writing, but form is not prescribed.
- Signature not required.
Request for Limitations

• Individuals may request specific restrictions on use and disclosure
• Covered entity required to agree if restrictions are for payment or health care operations (new under HITECH)
• If for treatment, covered entity can deny
• Patient right to request to inspect records
• Addressed above
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
Practice required to track all disclosures of PHI EXCEPT for disclosures:
- For TPO
- To the individual
- Incidental
- Pursuant to authorization
- Those that allow only opportunity to agree

Examples: disclosures for public health, required by law, pursuant to court order
• Right to an access report on who has accessed electronic PHI including access for purposes of TPO
  - by Jan 1, 2013 or 2014 depending when EHR adopted)

• Right to an accounting of the disclosure of paper or electronic PHI for certain purposes other than for TPO

• Proposed rules, not finalized
• PHI may be disclosed to a Business Associate if the Covered Entity has executed a Business Associate Agreement with the Business Associate

• HITECH extends all HIPAA requirements directly to the Business Associate
  - E.g. must have all policies, procedures & safeguards in place
  - Must modify agreements
  - Now subject to HIPAA civil & criminal penalties
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 Attorney Generals 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”)
HIPAA Security Rule

• To ensure confidentiality, integrity & availability of electronic PHI

• Unlike HIPAA privacy rule, issues are more technical than legal; emphasis on flexibility & tailoring to needs

• Required standards
  - Physical safeguards (e.g. access control, workstation security)
  - Technical safeguards (e.g. automatic logoff, encryption)
  - Administrative safeguards (e.g. password management, data backup plan)
  - Organizational requirements (e.g. updated business associate agreements)
  - Policies & procedures & documentation requirements
  - Disaster recovery planning
Breach Notification (HITECH)

• Three-step analysis:
  - Was there impermissible access to, use of, or disclosure of unsecured (not encrypted or destroyed) PHI?
  - Was access/use/disclosure in violation of HIPAA Privacy or Security Rules?
  - Was there significant risk of financial, reputational or other harm?
Breach Notification (con)

• 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 (con)

• 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

• Document in accounting

• Further requirements if SSN, credit card or other sensitive info disclosed or if 500+ individuals
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
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
jbarnard@mainemed.com