HIPAA & Privacy Compliance Update

Vermont Medical Society

FREE Wednesday Webinar Series
March 15, 2017

Anne Cramer and Shireen Hart
Primmer Piper Eggleston & Cramer PC

acramer@primmer.com
shart@primmer.com
(802) 864-0880

Agenda

- HIPAA and Vermont privacy law:
  - Critical concepts/key compliance steps
- Emerging HIPAA compliance challenges
- HIPAA audit program
- Recent enforcement actions
- Q and A

PRIMMER

Federal Law = HIPAA

- HIPAA privacy and security rules.
- Provide a "floor" for protecting the privacy of identifiable health information.
- Do not preempt state laws which are more protective of privacy or provide greater patient rights to access information.

PRIMMER

Vermont's Privacy Laws

- Patient Privilege, 12 V.S.A. § 1612: greater protection than the HIPAA privacy rules, allowing disclosure only with patient consent or as required by law.
- Vermont Health Care Privacy Law, 18 V.S.A. § 1881: allows disclosures permitted by HIPAA.
- Vermont Bill of Rights for hospital and nursing home patients, 18 V.S.A. § 1852 and 33 V.S.A. § 7301.
- Vermont Mental Health Disclosure, 18 V.S.A. § 7103

Vermont's Privacy Laws (cont.)

- State law is a "hodge podge."
- Recommendation: Have patients execute a general consent authorizing the provider to disclose PHI for treatment, payment, healthcare operations and coordination of care purposes. This consent should be retained in the patient's medical record.

PRIMMER

Protection of Health Information

- Categories:
  1. State law: no clear definitions
  2. HIPAA:
     a. Protected Health Information (PHI)
     b. Designated record set
     c. De-identified health information
     d. Limited data sets
  3. 42 CFR Part 2: Any information identifying treated individual or services provided at federal program for substance abuse treatment

Protected Health Information (PHI)

- Individually identifiable health information -- written, oral or ePHI
- Created or received by Covered Entity (CE)
- Relates to past, present, future physical or mental health or condition, or to provision of health care or payment for health care
- Excludes education records (FERPA) and employment related records

PRIMMER

Designated Record Set

- Group of medical records and billing records maintained by CE or used by CE to make decisions about individuals
- Significance?
  - Patient access rights
  - Quality review, payer requests, records in litigation
  - Distinguish business records, medical equipment printouts, scheduling information

PRIMMER

De-Identified Health Information

- Removal of list of identifiers required (names, geographic locators, age, dates, SSN, contact information, medical record and identifying numbers, image, biometrics).
- If de-identified fully, not protected and can be shared.
- Distinguish redacted records (name removal): still subject to HIPAA.
- If Limited Data Set (certain identifiers removed) can be shared for research, public health or health care operations under Data Use Agreement.

Who Must Comply with HIPAA Privacy and Security Rules?

- Covered Entities (CEs):
  - Health care providers
  - Health plans
  - Health care clearing houses
- Business Associates:
  - Independent contractor who
    - Performs function or activity for CE involving PHI
    - Must be under a Business Associate Agreement ("BAA")
- Business Associates of Business Associates

Use and Disclosure of PHI

- A CE may use and disclose PHI for treatment, payment and health care operations (TPO) without patient authorization
- Distinguish:
  - Consent needed under state law
  - Part 2 consent if federal substance abuse treatment program

HIPAA Key Concept: Minimum Necessary

- **Minimum Necessary Standard** limits uses, disclosures and requests for PHI to **minimum necessary amount of PHI** needed to carry out purpose of use or disclosure AND to limit disclosure to individuals with **need to know**
- Does not apply for treatment purposes or as directed by patient authorization

PRIMMER

Compliance Responsibilities for CEs

- Provide patients Notice of Privacy Practices (NPP)
- Adopt clear compliance policies and procedures
- Workforce training (no less than annually)
- Security measures and Security Rule Compliance
- Risk assessments (and implement response)
- Report breaches

What is a Breach?

- Unpermitted acquisition, access or disclosure of **UNENCRYPTED** PHI which compromises security or privacy of PHI
- Presumed, unless actual risk analysis pursuant to rule shows low probability of "compromise"

PRIMMER

Breach Reporting

- Notify individual within 60 days.
- Notify HHS and media if over 500 people affected.
- Annual notice or log to HHS of breaches.
- If personal financial information (SSNs or financial accounts), notice to Vermont Attorney General in 14 days and individual within 45 days. 9 V.S.A. § 2435.

PRIMMER

Patient Rights Under HIPAA

- Access/copies in 30 days
- Copies for reasonable, cost-based fee (labor, supplies, postage)*
- Request to amend or state disagreement
- Request accounting of access
- Request restriction (if self-pay, may prohibit insurer's access)
- Communication choice

*will preempt Vermont Law, 18 V.S.A. § 9419, in part, except free copy for SS Act claims

PRIMMER

Emerging HIPAA compliance challenges

- Ransomware
- Texting patients
- Emailing patients

PRIMMER

Ransomware

- Type of malware (malicious software).
- Attempts to deny access to a user's data by encrypting it.
- Directs the user to pay ransom to the hacker in return for a decryption key,
- May also destroy or exfiltrate data.

PRIMMER

Ransomware = HIPAA breach?

- Whether ransomware is a breach under the HIPAA Rules is a fact-specific determination.
- When ePHI is encrypted by a ransomware attack, a breach has occurred.
- Unless the covered entity or business associate can demonstrate a "…low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred.

Ransomware – what should you do?

Implement:

- A **security management process**, including:
  - conducting a **risk analysis** to identify threats and vulnerabilities to ePHI, and
  - security measures to mitigate or remedy those identified risks;
- Procedures to guard against and detect malicious software;
- **Training** for users on malicious software protection, so they can assist in detecting malicious software and know how to report such detections; and
- **Access controls** to limit access to ePHI to only those persons or software programs requiring access.

FACT SHEET: Ransomware and HIPAA
https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

PRIMMER

Text Messaging

- Generally not secure because:
  - messages lack encryption;
  - sender does not know with certainty the message is received by the intended recipient; and
  - telecommunication vendor/wireless carrier may store the text messages.

Texting Recommendation

Before texting, we recommend:

- perform a risk analysis, or
- use a third-party messaging solution that establishes a secure communication platform.

PRIMMER

Texting: Written Agreement

- Get a signed agreement from the patient.
  - Patient agrees to accept communication by text;
  - The types of information texts may contain;
  - Password and encryption standards for the devices that are used;
  - Addition of texts to medical record;
  - How and when texts are deleted;
  - What type of information patient agrees to transmit or receive by text; and
  - Must notify practice if phone number changes or phone is lost, etc.

Email Best Practices

- If a patient emails you, you may assume that email is an acceptable form of communication for the patient.

- BUT, if patient may be unaware of risks of using email, alert them to risks and let them decide whether to continue

  (risks: work email - who can access it?, email could become part of medical record, never use email in emergencies, etc.).

PRIMMER

Email Best Practices (cont.)

- For the first communication, double-check the email address.
- Send an email alert first, so patient can confirm correct address.
- Limit amount/type of medical information being disclosed.
- If patient copies a third person on email, only reply to the patient.

PRIMMER

HIPAA Audit Program

- HITECH requires the US government (Health and Human Services - HHS) to perform periodic audits of covered entities and business associates.
- HHS Office for Civil Rights (OCR) enforces HIPAA and HITECH Rules.
- For audit information, see:

http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html

PRIMMER

Audit Program Objectives

- OCR uses audits to **identify best practices and discover risks and vulnerabilities** undetected through OCR's ongoing complaint investigations and compliance reviews, and enable OCR to get out in front of problems before they result in breaches.

- OCR will identify best practices gleaned through the audit process and provide guidance targeted to identified compliance challenges.

HIPAA Audit Program Phase I

2011 - 2012

Audited controls and processes of 115 Covered Entities to comply with Privacy, Security and Breach Notification Rules.

PRIMMER

HIPAA Audit Program Phase 2

- Launched in 2016.
- Reviews Covered Entities'/Business Associates' policies and procedures.
- Desk audit: very little on-site.
- Started with an email asking to verify email address and contact information.
- Followed by pre-audit questionnaire.

osocraudit@hhs.gov

If you did not get an email, check junk and spam folders for OCR emails.

PRIMMER

Alert: Phishing Email Disguised as Official OCR Audit Communication - November 28, 2016

Phishing email originated from OSOCRAudit@hhs-gov.us and directed individuals to a URL at http://www.hhs-gov.us.

Subtle difference from the official email address for HIPAA audit program, OSOCRAudit@hhs.gov and the website, http://www.hhs.gov, typical in phishing scams.

PRIMMER

Most Investigated HIPAA Compliance Issues for Private Practices

- Impermissible uses and disclosures of PHI.
- Lack of safeguards of PHI.
- Lack of patient access to their PHI.
- Use or disclosure of more than the minimum necessary PHI.
- Lack of administrative safeguards ePHI.

PRIMMER

Case Examples of Enforcement Actions Against Private Practices

- Improper charges for medical records.
- Providing summary record instead of full record set without consent.
- Refused access to medical exam records when paid for by third party.
- Denial of portion of record created by different provider.
- Denial of records to patient with balance due.

PRIMMER

Other Examples of Common HIPAA Enforcement Actions

- Stolen laptop, flash drive, phone . . .
- Failure to enter into business associate agreements.
- Failure to disclose minimum necessary for all but treatment purposes.
- Waiting rooms – computer monitors, sign-ins, privacy protections, etc.
- Proof that Risk Analysis has been performed.
- Timely breach notifications (60 days)

HIPAA Enforcement Best Practices

- Conduct annual security risk analysis and respond to results.
- Investigate, provide notice of, and report breaches.
- Update and maintain BAA checklist.
- If ever contacted by OCR, OSOCRAudit@hhs.gov, immediately review and revise policies and procedures if need be. Post-incident amendments and revisions to policies must be accurately dated.

Questions?

Vermont Medical Society

FREE Wednesday Webinar Series
March 15, 2017

Anne Cramer and Shireen Hart
Primmer Piper Eggleston & Cramer PC

acramer@primmer.com
shart@primmer.com
(802) 864-0880