HIPAA Ready: Changing polices one at a time

MUNSON MEDICAL CENTER
MUNSON HEALTHCARE

Purpose of Today's Presentation

- Key areas of change
  - What's new and what's different
- Implications of removal of "Harm Thresh-hold"
  - More reportable breaches
- Guidance and Recommendations for compliance
  - Due date is 4 months away.

Benefits of Knowing New Regulation

- Avoid inadvertent breach
- Avoid disciplinary consequences and negative light on your agency.
- Be a resource to others

Notice of Privacy Practice

Must “post” and offer

Patients signs and dates

Need only offer 1x

Is agency specific

Must have NPP available

NOPP Must have these changes:

- Prohibition of sale of PHI without a signed authorization
- Right to opt out of fundraising efforts mailings or calls
- Right to restrict disclosure to Health Plan for out-of pocket payments
- Duty to notify patient in case of a breach

NOPP Must have these features

- Description of the types of use and disclosures that require authorization, and
- Any disclosure not describes in NOPP will not be made, unless authorization given.
- Remove statement re provider may send info re tx alternatives or health products (paid by 3rd party)
- All new patients after 9/23 must receive new NPP

Incident Management Policy

Breach Notification
No long based on "significant risk of harm"

No longer exception for loss of a data set without zip codes or DOB

- Now, presumption of reportable breach, unless can demonstrate low probability PHI "compromised."

Risk Assessment

- Must be formalized, not "ad hoc" and documented - to show analysis as to why to notify patient or not.
- Compromised means "PHI inappropriately viewed, accessed, re-identified, acquired, or re-disclosed.

Required

- Entities must conduct risk assessments following all PHI privacy or security incidents.

Risk Assessment

- Does the access, use or disclosure violate HIPAA Privacy?
- Was the PHI "secured" or "unsecured"?
  - Secured means encrypted or shredded.
- Does an exception to breach apply?

Show low probability of compromise?

Exceptions

- Unintentional acquisition by workforce member
- Inadvertent disclosure between authorized persons and not re-disclosed
- Good Faith belief person could not reasonably retain PHI

Required Risk Assessment

- Nature and extent of PHI, and likelihood of re-identification;
- The unauthorized person who accessed and to whom was PHI was disclosed?
- Was the PHI acquired or viewed?
- Extent the risk to PHI been mitigated?

Factor One: Nature and Extent

- PHI sensitive in nature?
- Financial, credit card, SSN or DLN?
- Risk of ID theft?
- Amount of clinical
- Potential for harm
- Value to others?

Mitigation

- What steps have been taken to mitigate risk to PHI
  - Item recovered or found?
  - Item "remotely wiped?"
  - Item returned? Unopened?
- Security Rule: Assess risks and manage risks

Breach Notification

- Duty to report breach to patient <60 day
- Duty to inform Health and Human Services at year's end if <500
- Inform HHS within 60 days if >500
- Duty to document details, analysis, and conclusion
- Inform Admin if over >25 affected

What are the dangers and challenges?

Why investigation is important

- Lost PHI *presumed* to be *compromised*
- When is "low probability" demonstrated?
- OCR views disregard as "willful neglect"
- Strong incentive to over report.
- Creates major exposure for CE for audit

Risk Assessment tool

- Must be "formal" and not ad-hoc
- Must ask and answer 4 factors, minimum
- See handout
- Sanctions policy at Munson revised to put employees on corrective action
- for reportable breaches.

Fundraising and Marketing

Fundraising

- New HIPAA rule adds categories of PHI that may be used or disclosed:
  - Department of service
  - Treating physician
  - Outcome information
  - Health insurance status

Marketing

- Is the communication about a product or service that encourages purchase or use? If yes, marketing
- Describes health item/service offered by CE or another? Not marketing.
- Remuneration received from 3rd party whose item or service is described? If yes, is marketing; get authorization

Sale of PHI

- CE may not receive remuneration in exchange for PHI
- Exceptions covered in marketing policy

Records Release

Decedent Information

- PHI no longer protected under HIPAA 50 years after death.
- (Typically released to "executor of estate" or use special form for inheritance issues).
- CE may now disclose PHI to persons involved in decedent's care or payment if not contrary to prior expressed wishes

Copy to 3rd Party

- Patient may designate 3rd party to receive copy of records:
  - Must be in writing
  - Must clearly identify the person
  - Must clearly identify where to send copy

Student Immunization Record

- May release to school without authorization:
  - If state law requires school to have record
  - Written or oral agreement given (and this must be documented)

Disclosure Policy

- Staff may disclose PHI to friends and family involved in care or payment, of deceased.
- Purpose is to better help family understand/process cause of death
- Family definition is broad and is not limited to bio-relations.

Restriction of Disclosure

- **You must accommodate** patient request to restrict disclosure to health plan if:
  - Patient or another pays **out of pocket** (in full) prior to service or treatment
  - Disclosure is not required by law
  - May request that request is put in writing

Medicare Exception

- If Medicare, then the physician or supplier must submit a claim to Medicare.
- However, there is an exception to this rule where a beneficiary (or the beneficiary's legal representative)
- refuses…to authorize the submission of a bill to Medicare. In such cases, a provider is not required to submit a claim to Medicare for the covered service and may accept an out of pocket payment.

Minimum Necessary

Disclosure policy

- Note that disclosure of more than is minimally necessary is a breach that may be reportable to patient and HHS

Research – Last policy chanage

Research

- May combine "conditioned" and "unconditioned" authorizations on same form.
- Unconditioned authorization for opt in must be by check box or signature line
- Authorization may govern future research and inform of potential for future research.

Question and Comments

- Please feel free to contact me to discuss any privacy issue.
- Rochelle Steimel
- rsteimel@mhc.net
- 231-935-5765