HIPAA

New Breach Notification Risk Assessment and Sanctions Policy

MUNSON MEDICAL CENTER
MUNSON HEALTHCARE

Incident Management Policy

For breaches affecting

1-3 individuals

+25 individuals

+ 500 individuals

Focus on:

-analysis
-documentation
-PHI recovery
-remediation
-prevention of re-occurrence
-sanctions

Important Exceptions to a Breach

- Unintentional access or use, made in good faith, within scope, and no further disclosure.
- Inadvertent disclosure to another in same CE and no further disclosure.
- PHI disclosed to recipient who would not retain the information.
- PHI is encrypted or shredded.

Assess "Low Probability" of compromised PHI

- Type of identifiers?
- Nature and extent of PHI?
- Who is the unauthorized person?

  Who learned of the PHI
- Was the PHI printed out, or viewed?
- Has the extent of risk been mitigated?
- Is there financial/legal benefit with the breach

How sensitive is the PHI

- How likely is re-identification?
- SSN or DLN?
- How many patients affected?
- How much PHI?
- Psych hx, medication use, alcohol or drug use, HIV, etc.

Risk Assessment Guidelines

- See handout re:
  - -identifiers
  - -encryption
  - -exceptions
  - -risk assessment
  - -burden of proof
- Lower Risk versus
- Higher Risk to **PHI**
- note: no longer an assessment of harm to patient, but new focus on safety of **PHI.**

Breach Notification Letters (see template)

- What happened
- What PHI was compromised
- By who, when and how?
- Action steps being taken to prevent reoccurrence
- Public Relations opportunity to reassure re privacy priority

Remediation and Preventing Re-Occurrence

- Offer credit monitoring
- Set up a call-center
- Improve policy
- Add staff training
- Encrypt portable media
- Require new password
- Increase physician security eg. Locks
- Sanctions to employee
- ID gaps in compliance

Sanctions: 1st level

- Low Risk of compromised PHI and no harm to patient or organization
- No Breach Notification required
- Verbal warning with
- re-education or a process improvement

Sanctions: Low risk but Intentional access

- Written warning or final written warning
- Low Risk but malicious or unethical intent such as a domestic dispute, or flagrant disregard for policy:
- Termination

Sanctions #2 Moderate risk of compromise

- Unknown harm to patient or organization
- Breach Notification required
- Access could be an inadvertent mistake, intentional or malicious
- Written warning or Final written warning
- Termination possible

Sanctions #3 Multiple patients/PHI/major harm

- Breach Notification required to:
  - Administration
  - Patients
  - Media if over 500
  - HHS if over 500
  - (posted on HHS Web)
- Unintentional (device lost or stolen)
- Intentional or
- Malicious/Unethical/ Personal Financial gain/disregard for policy:

Termination

Documentation Requirements

Have you followed your sanctions policy?

Has HR and the manager thoroughly addressed the matter to prevent re-occurrence?

- "Does the punishment fit the crime"?
- What is your resolution?
- Your conclusion and gaps identified?

Documentation Requirements

- Complainant name, contact info
- What PHI compromised?
- How many affected?
- Date of breach and date discovered
- Answer to all risk assessment questions
- Who was consulted?
- How was your conclusion reached?
- Date of letter to patient

Documentation

- See HIPAA toolbox for documentation checklist.
- Remember more breaches will be reported and all must be documented
- Exception: You may decide to send letter and notification without an analysis, but must error on side of over-rerporting, and still document.

Fines

HIPAA is enforced by the Office of Civil Rights, within the Dept of Health and Human Services

Anyone can enter a complaint on the OCR website

- Even if agency "did not know" it was a violation $100 to $50,000.
- Note: individuals and the organization can be fined.

OCR Complaint Statistics

- Roughly 1000 new HIPAA complaints are received by OCR each month
- As of 6 months ago (12/12) there were 525 cases violations over 500, and 60,000 under.

HIPAA fines are higher

- OCR conducts audits on regular basis
- May pose a $1000 to $50,000 fine for violations found
- Fines increase if violation is due to "willful neglect" such as lack of encryption standard, or lack of policies, to $10,000 to $50,000.

Willfull Neglect

- Conscious, intentional failure or reckless indifference
- OCR will investigate all cases of willful neglect
- OCR will impose fines for all willful neglect
- OCR fines are $50,000 for violations due to "willful neglect" not corrected within 30 days.

OCR Fines and Penalties

- Penalties are capped at $1.5 million for identical violations during the year.
- New Criminal penalties include 1-10 year jail terms.
- Example:
PHI sold for financial gain or malicious harm (fraud or ID theft etc)

OCR Audits

- OCR now has a permanent audit program
- Audits address privacy and security
- OCR uses fines collected to fund more audits
- With greater use of EMR, more possibility of misuse for fraud or ID theft exists; thus more audits and fines

All Subcontractors and vendors now a BA!

- They must notify you of a breach notification.
- Are now a covered entity under HIPAA
- Vicarious liability for business associates

Create Large Scale Incidence Response Team

- HR, legal, physicians,
- Office manager, privacy officer and Munson Security.
- Munson Privacy Officer available for consultation.
- Assemble and practice a case scenario.
- Create a thorough policy on how to handle small and large scale breaches, investigations, documentation, analysis and mitigation

Staff Education

- To prevent breaches, the best approach is clear and frequent HIPAA education and tips and discussions.
- "Scare people straight."
- Make consequences clear and quick.
- Let them know you "trust but verify".

Thank you!

- Rochelle Steimel, OTR, MPH
- Privacy Officer
- rsteimel@mhc.net
- 935-5765