MUNSON MEDICAL CENTER

MUNSON HEALTHCARE

Northwest MMBA Conference 2013- Participant Handout

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

Benchmark Study on Patient Privacy

***More healthcare organizations are having _____.** Many health care organizations struggle with a lack of technologies, resources and trained personnel to deal with privacy risks.

Technologies that promise greater productivity and convenience such as mobile devices, file-sharing application **are difficult to secure**.

***_____ _____ continues to be at the root of the data breach**. The primary cause of large scale breaches are a lost or stolen computing device. But breaches affecting less than 500 people is caused by employee mistakes and negligence. Thirdly, criminal attacks are increasing.

Medical Records,_____ and Insurance records are the types of patient data lost or stolen most often. What is PHI? Patient names, telephone, DOB, SSN, MRN, Account numbers, DLN, all chart information.

Data breaches can have severe economic consequences. Average impact over past 2 years in this study is $2.4 million! for breaches investigated by the OCR. Several breaches costing more than $500,000 have increased 48% of healthcare organizations in 2010 to 57% of respondents to this study.

Purpose of Presentation

1. How to be HIPAA compliant in this environment?
2. What patient rights have been strengthened?
3. What are best approaches to take?

Billing Department Environment

_____ _____ skills and knowledge re HIPAA will assist you.

II Fundamental principle for HIPAA compliance

Disclosures are allowed for 3 major exceptions: T_____, P_____ and O_____.
Billing comes under Payment.

Note that on the Authorization for Treatment and the Notice of Privacy Practices that patients are offered when they register for treatment, it tells patients that their medical information will be shared with their insurers "for the purposes of determining insurance coverage and billing, claims management, and reimbursement." Their medical information may be disclosed to any insurance company, third party payer, third party administrator, collections agency, health plan or other health care provider involved in the payment of their medical bill and will include excerpts from their medical record.
So you have a _____ right to disclose and share information for sake of payment.

III Overview of HIPAA Omnibus Rule Changes: What's New?

1. _____ threshold for reporting breaches to patients and HHS.
   a. Past: Threshold of harm.
   b. Has the PHI been compromised?
   c. Effective **Sept 23, 2013** breaches of PHI must be reported to patient within 60 days, and to HHS at end of year. Primary examples: inappropriate access to PHI, verbal disclosure to person who does not have job related need to know, wrong disposal of PHI or unsecured errors in mailing, fax, text, pages, social media, phone message, emails, or loss of mobile device with PHI.
2. Definition of reportable breach has changed! Before, a **threshold of harm** to patient had to be reached, for emotional, financial, legal or reputational harm. Now, a reportable breach is PHI that has been "_____" which means PHI has been accessed, viewed or acquired by someone without an appropriate need. If your agency can't prove that it hasn't been compromised, then it is a reportable breach.

By law, each covered entity under HIPAA must_____the patient if a breach of unsecured PHI occurs.
The one safe harbor in this is the use of _____or shredding. If the person receiving the PHI cannot access or decipher the PHI then it is not a reportable breach.

3. Able to discuss facts of death with loved ones to help explain, if patient did not express wishes for confidentiality re diagnosis. Record release is still guided by Executor or Estate or special release form for purpose of collecting insurance death benefit.

4. New Notice of Privacy Practices, letting patients know they will be notified if a breach of their information occurs and that they can opt out of any fundraising letters/calls.

   Visit www.munsonhealthcare.org/HIPAA for template of NOPP, educational materials, compliance issues, complaint management and FAQs/posters etc.

5. Right of patient to request that their_____not be notified of treatment or service, IF they pay in full (out of pocket) prior to delivery of service. Get the request in writing and (somehow) flag that record for billing and for future audits.

6. The Privacy Officer or Office Manager must do a Formal _____ _____ .questions must be asked and documented and used to determine if PHI has low risk or high risk of compromise:

Risk Assessment, continued:

a. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
b. The unauthorized person who used the protected health information or to the disclosure was made;
c. Whether the protected health information was actually acquired or viewed; and
d. The extent to which the risk to the protected health information has been mitigated.

Breach Exclusions:

e. Any _____acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
f. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is _____ _____used or disclosed in a manner not permitted under the Privacy Rule.
g. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to - _____such information

IV HIPAA compliance on a day to day basis:

1) Keep access to records restricted to a **_____ _____need to know**. No access out of _____or concern, or to keep tabs on extended family members, children, or ex husband etc. This includes all the various software programs you may use for medical information, registration and billing.

2) Disclose patient information to others at work who have a job related need to know. Avoid any reputation as someone who gossips or shares. Breach example: "I see your sister was here for a biopsy."

3) Verify _____of caller. Put the burden of proof on the requestor of information. Ask them to fax or mail the legal papers, or put their request on letterhead. Ask them their relationship to patient. Ask to talk to patient.

4) Disclose the_____amount of information needed…the financial data and not necessarily the medical information. How do you handle this?

5) Obtain patient verbal (verbal is fine) or written permission to disclose to those not listed as guarantor/responsible for payment. Call the patient, and document their response. Or use best judgment, and document "in the _____ _____ of the patient" you disclosed WHAT to WHO, WHEN, for purpose of …… tax purposes. Disclose in best interests of patient. Patients themselves always have a right to their financial and medical records.

Patients have a right to request _____ communications, such as a work phone, or an alternative address. If this request is known and not honored, then it is a HIPAA violation.

Best Approaches with Customers

1. Give yourself time to _____. Step back and talk to a co-worker or supervisor about it. Plan your response. Call Privacy, or supervisor if needed. For example, a lawyer is calling to ask for the billing record so that in court, he can ask that for restitution for medical expenses. Or an ex-husband is calling to learn of wife's medical bills. What would you do?

2. You are not responsible for knowing if patients are divorced or if there is discord, if they have not notified your office or if there is no notation or paperwork in the chart. You are going by guarantor listed. The patient is responsible for updating the guarantor information and you may assist in that process.

3. Avoid _____ the patient. Keep them informed. Surprised patients complain.

4. Get out of the _____ where ever possible. When a 3rd party asks for information, talk directly to the patient when possible.

5. In general, ask for all requests for information on _____signed and dated, explaining what they want and the rational for their request. A phone call is hard to prove.

6. _____the patient's response or your attempt to contact patient, or condition of patient that makes it impossible to obtain her opinion.

7. Use your best judgment and do what feels reasonable. If HIPAA is interfering with your job performance, it is possible that you are interpreting HIPAA too strictly. HIPAA is not meant to interfere with your job. Document how you reached your _____conclusion, and acted in the best interests of the patient. For example is this caller going to help pay the bills for patient?

8. Communicate and keep PR with caller but point out HIPAA privacy rules.

9. Anybody can complain re privacy, just as anyone has the right to sue, however, good practices on your part can deflect blame and show reasonable measures used. When mistakes are made, an _____, made in a timely manner is most often exactly what patients want.

Other Best Approaches for Avoiding Privacy Breaches

1. Use Fax cover sheet with confidentiality statement, every time.
2. Encrypt all email with PHI going outside of password protected system.
3. Verify identity and disclose minimum necessary information.
4. Do not access charts unless job related need, and supervisor agrees.
5. Protect your mobile device, ipads, smart phones, pagers with encryption and passwords.
6. Dispose of PHI in confidential bins or shredders.
7. Use encrypted thumbdrives.
8. Check fax numbers for accuracy.
9. Plan for "worst case scenarios" in policy and practices. Cover bases for what to do when things go wrong. (example: courier service in accident while carrying 100 paper charts.)
10. Auditing software more sophisticated now in larger hospitals, example Fair Warnings detects same name access.

Thank You! Call or email if questions, 231-935-5765 or rsteimel@mhc.net

Visit www.munsonhealthcare.org/HIPAA