Establishing and Implementing a Process to Investigate and Resolve Privacy Breaches and Complaints

Barbara Seitz, RHIA
Privacy Officer/Director of HIM
South Peninsula Hospital
Homer, AK

Becky Buegel, RHIA
Privacy Officer/Director of HIM
Casa Grande Regional Medical Center
Casa Grande, AZ

OBJECTIVES

At the End of This Presentation, Participants Should:

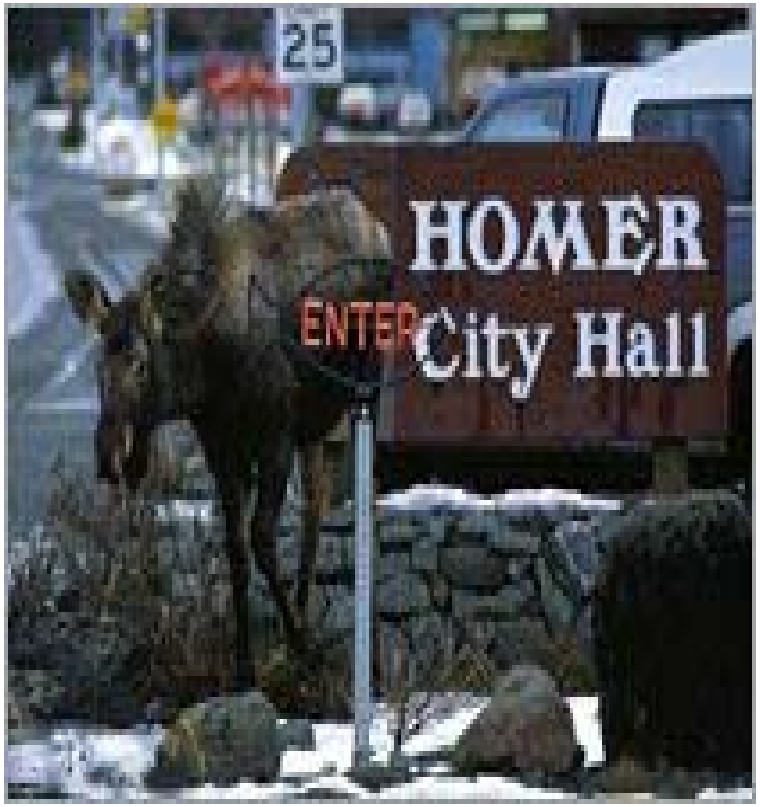
- Be able to identify at least three items that the Privacy Rule does and does not require when responding to complaints;
- Have an understanding of the Privacy Complaint Process at South Peninsula Hospital.
- Know what the acronym FMEA means.
- Understand the FMEA approach to identifying and preventing privacy breaches before they occur.

The Privacy Rule Requires

- Covered Entities to develop a process to receive complaints about:
  - Policies & Procedures
  - Compliance with Policies & Procedures
  - Overall compliance with the Rule

An individual may file a complaint with a Covered Entity (CE) as well as the HHS Secretary.

- The goal is to ensure accountability of CE policies and procedures and to ensure compliance with the Privacy Rule
- The HHS will allow CE to respond to complaints in an appropriate and timely manner



HSS Complaint Continued

- If complainants contacts HSS the CE will be subject to the Secretary's Compliance Investigation.
- Once on site, investigators can investigate any aspect of the CE's HIPAA compliance.

When writing your policy and procedure, CE's should consider:

- Requirements for internal complaint process, Section 164.518 (d).
- How a complaint will trigger other issues under the Privacy Rule.
- How the internal process relates to complaints to the Secretary of HHS.
- What are the foreseeable areas of concern?

The Privacy Rule “DOES NOT”

- Offer a description of a required process to address complaints;
- Require CE to acknowledge receiving a complaint in writing;
- Define a complaint;
- Require a written complaint;
- Define a “reasonable time” in which to respond;
- Require CE to notify patients of improper disclosure.

The Privacy Rule Requires CEs to:

- Develop a Complaint Process;
- Retain complaint log for period of 6 years;
- Appoint contact person to receive complaints;
- Develop a standardized complaint form;
- Mitigate harm arising from noncompliance;
- Protect complainant from retaliation;
- Include process in Notice of Privacy Practice;
- Develop and apply Sanctions P&Ps.

Complaint Process for SPH

- HIPAA team determined who would investigate and respond to complaints based upon:
  - Nature of complaint
  - Focus
  - Scope
- Team investigated preemption of state privacy laws. (45 CFR 160.202/203)

“WHO” should be responsible for processing HIPAA related complaints?

Privacy Officer?

HIM professional?

Risk Management?

Security Officer?

Compliance Officer?

Legal counsel?

Patient representative team ?

Make sure you communicate who is chosen and have a back up person to take complaints!

Determine Level of Involvement

- **Level 1** – An issue that you/designated person can handle yourself and resolve in a short period of time.
  - i.e. misdirected lab result within the facility

Involvement (Continued)

- **Level 2** – Issue involves the attention of other staff members.
  - i.e. Two employees discussing PHI with each other on campus.

You/designated person meet as a group with involved staff, managers and HR rep.

Involvement (Continued)

- **Level 3** – Serious issue or security incident. Organize an incident response team to determine:
  - harm to patient
  - patient relations
  - legal implications
  - law enforcement

Security and Privacy Officers should be trained on how to handle the media in situations like this!!

Complaint Investigation should generate an audit trail:

- Complaint form;
- Periodic report on status of investigation;
- Disposition form - Root Cause analysis
  - Identify privacy deficiencies
  - Identify appropriate Corrective actions to take;
- Final report for the complainant;
- Disposition form – final record for reporting.

WARNING, WARNING, WARNING

- Standardized wording to claim privilege of non-discovery for civil liability should be written into your policies.

To Tell or Not to Tell…….

- HIPAA Privacy Rule **does not** require CE to inform patient of improper disclosure of PHI.
- SPH philosophy: Admitting a mistake shows "Good Faith."
- Breach must be entered into the Accounting of Disclosure log regardless if you inform the patient.
- Helps comply with requirement that you Mitigate (lessen ant harmful effects caused by the privacy violation.)

Disclosure Accounting Log

- Required to document improper disclosure and violations of rule;
- Retain for a minimum of 6 years per federal or state retention requirement;
- Does not include incidental uses and disclosures (August 2002 modification)
  - Cannot reasonably be prevented;
  - Is limited in nature;
  - Occurs as a by-product of an otherwise permitted use or disclosure.

Complaint Form should include:

- Name of complainant;
- Date & time complaint is filed;
- Date & location of incident;
- Location;
- Persons involved;
- Nature of breach.

Complaint Form (Continued)

- Harm, if observed;
- Statement by suspect & witnesses;
- Who was notified;
- Remedial action taken, if any;
- Recommendations for Corrective Action.

Duty to Mitigate

- Entities have a duty to mitigate any harmful effect of a use or disclosure of PHI that is known to the CE.
  - This duty is applied to a violation of the CEs P&Ps, not just a violation of the requirements of the regulatory subpart.

Retaliation

- Regulations prohibit retaliation against an individual for filing a complaint with the HHS Secretary as well as any other person who files a complaint with the CE (i.e. staff and providers.)
- Allowances exist for whistleblowers and crime victims who disclose PHI. (See 164.502(j).
  - Made in good faith;
  - Disclosure is made to a public health authority, health oversight agency, attorney, or health accreditation organization.
- This provision applies to the Privacy Rule alone – not to all the HIPAA Administrative Simplification rules.

SANCTIONS

- CMS requires CEs to develop and apply, when appropriate, sanctions against its staff and providers who fail to comply with Privacy P&P or with the requirements of the rule.
  - Appropriate to the nature and scope of the violation.
  - Sanctions can range from a verbal warning to termination.

Conclusion

- The best practice for avoiding a complaint by an individual to the Secretary is to implement a responsive process and good documentation practices.
- Complaint process should help your organization do a better job of protecting patient privacy, not just comply with HIPAA regulations.

FMEA

- **F**ailure
- **M**ode
- **E**ffect
- **A**nalysis

What is FMEA?

- According to the Veteran's Administration National Center for Patient Safety, a Failure Mode Effect Analysis is a systematic method of identifying and preventing product and process problems *before* they occur.

FMEA is *not* a new process.

- Developed by the US Military in 1949;
- Used to identify the effect of system and equipment failures before they occur;
- Also used in the automotive and aerospace industries.

FMEAs

- Are often used to analyze a bad experience or near-miss situations;
- Are most effective when used as a part of the design process and *not* after the process has failed.

Select a HIPAA-Related Process

- Processing requests for PHI
  - Insurance underwriting
  - Legal cases
  - Patient's representative
- Case Management
  - Concurrent Reviews
  - Retrospective Reviews
- Research Protocols from Other Institutions or Organizations

Evaluate the Risk of Failure for the Process You've Selected

- The risk of failure and its subsequent effect can be determined by three factors:
  - Frequency;
  - Severity;
  - Detectability.

FMEA 7 Step Process

1. Choose a topic.
2. Assemble a team.
3. Describe the process in detail.
4. Identify potential failures.

FMEA 7 Step Process (continued)

5. Rate the risk:
   - Frequency;
   - Severity;
   - Detectability.
6. Calculate the Risk Priority Number (RPN.)
7. Identify actions that can reduce or eliminate risk.

Choose a Topic

- Can be a previously identified problem.
- Could be something that in and of itself has been identified as a high-risk process.
- Remember to review existing policies and procedures.

Assemble a Team

- Involve people who perform the process every day; they are the experts, not the supervisors, managers, or directors.
- Have an impartial facilitator.
- Train the team in the FMEA process.

Describe the Process in Detail

- Flow-chart the process.
- Be as detailed as possible.
- Use flow-charting tools such as post-its, white boards, etc.
- Don’t rush this step.
- Keep focused and put aside issues that may arise but have nothing to do with the task at hand.

Identify Potential Failure Modes

- What are the various ways the process can fail to accomplish its intended purpose?
- In other words: Identify hazards that are of such significance that they are reasonably likely to cause a privacy breach (insert any process/problem) if not effectively controlled.

Rate the Risk - Frequency

How often will there be an adverse outcome?

(1) Remote - Highly unlikely it will ever occur.

(2) Moderate - It could happen sometime.

(3) Occasional - Probably will occur.

(4) Frequent - Very likely to occur.

Rate the Risk - Severity

(1) Minor – Minimal effect on the organization/ could be resolved internally.

(2) Moderate – Potential for complaint to OCR.

(3) Major – Potential for litigation/lawsuit.

(4) Catastrophic – Criminal/civil charges & fines.

Rate the Risk – Detectability

(1) Certain to Detect – Problem/breach always detected (9/10)

(2) Might Detect – Problem/breach likely to be detected (5/10)

(3) Probably Won't Detect – Problem/breach unlikely to be detected (2/10)

(4) Can't Detect - Not possible to detect (0/10)

Calculate the Risk Priority Number

Frequency X Severity X Detectability = RPN

Use the Risk Priority Number to rank and prioritize failure modes.

Identify Actions to Be Taken to Reduce or Eliminate Risk

- What changes can be made to the process?
- How can they be implemented?
- How soon can they be implemented?
- Follow up on changes to make certain they're effective.

Protect the Process

- Cite each page as confidential with intended privilege.
- Treat the same as any PI/QA or risk management process.

Practice FMEA

See separate handout.

Barbara's Resources/References

- Health Information Compliance Insider (HIMSS), www.brownstone.com
- In Confidence (AHIMA), www.ahima.org
- The Medical Management Institute
- Strategic Management Systems, Inc.

Becky's Resources/References

- *The Basics of Healthcare Failure Mode and Effect Analysis,* VA National Center for Patient Safety.
- *A "Proactive" Risk Strategy: Failure Mode Effect Analysis,* Ann Abke, Director of Risk and Compliance, St. Joseph's Hospital and Medical Center, Phoenix, AZ.
- *FMEA Selection Criteria and Opportunity Statement Worksheet,* Catholic Healthcare West.
- *Example of a Health Care Failure Mode and Effects Analysis for IV Patient Controlled Analgesia,* Institute for Safe Medication Practices.

Contact Speakers

- Barbara Seitz –bas@sph.org
- Becky Buegel – rbuegel@cgrmc.org

- Thanks for your time!

Denali / HIPAA – The BIG One