HIPAA Implementation

Practical Steps in Building a HIPAA Compliance Team and Implementing an Effective Compliance Program

Ann M. Bittinger, Esq.

Kutak Rock LLP

Kansas City, Missouri

The HIPAA Summit West, San Francisco, June 22, 2001

Goals for Presentation

- Discuss corporate acceptance of HIPAA privacy rules.
- Discuss choices for members of HIPAA Privacy Team.
- Discuss assessment methods.
- Address documents and policies needed.
- Discuss groundwork for on-going HIPAA compliance.

Two Keys to Keep in Mind

- HIPAA compliance is not “one size fits all.”
- Do what makes sense.
  - Comply with already existing duty to keep information private.
  - Keep in mind that confidentiality promotes patients’ health.

Step 1: Corporate Level Action

- Board of Directors Resolution that:
  - Directs officers to:
    - Hire a privacy officer.
    - Take steps to comply.
    - Assemble HIPAA Privacy Team.
    - Prepare policies and procedures.
    - Name the privacy officer, once hired.
- CEO Letter to Employees

Model Memorandum
[Content may be adapted into press release]

TO: All Hospital [Clinic] Employees

FROM: _____, CEO

DATE: _____, 2001

RE: Appointment of Privacy Officer and Development of Privacy Plan

It is my pleasure to announce that [hospital name] has appointed [name] to be the hospital's Privacy Officer. Protecting the privacy of patients' individually identifiable health information is one of the hospital's top priorities. The hospital is concerned with studies showing that patients do not disclose relevant health information to their physicians and nurses because, although they trust the physicians and nurses, they do not know what will happen to the information once it leaves the providers' hands. These studies, the promulgation of the HIPAA final privacy regulations and the belief that the protection of individuals' health information promotes patients' health has prompted the hospital to act to protect patients' health information.

[Privacy's officer's name]'s duties as privacy officer will include overseeing the creation and implementation of a state-of-the-art hospital privacy plan. To create the plan, [name] will be leading a team that will audit all current policies and procedures relating to the use and disclosure of and access to individuals' health information. Please cooperate with the team as its members are making their assessments. Employees' input will be solicited during this process.

As the privacy plan is being formulated and implemented, changes in the hospital's policies and procedures may be made. For example, the hospital will be required under the new federal privacy regulations to give a new type of privacy notice and get new consents and authorizations from patients pertaining to disclosure of their information. Also, all hospital employees must participate in training about the new regulations. We look forward to your cooperation with these changes and educational programs.

[Hospital name] plans to work expeditiously and effectively to formulate and implement its privacy plan in order to protect patients' health information. We look forward to [privacy officer's name]'s leadership in this effort.

Privacy Officer

- Who should it be? Various opinions:
  - Ideally, a new person whose job is privacy only.
  - Realistically, consider separating from risk management & fraud and abuse compliance.
  - Definitely give the person immediate access to CEO (high on the corporate structure).

Privacy Officer

- Circulate name and number for questions.
- Create a privacy bulletin board or intra-net site.

Privacy Officer

- Initial Tasks
  - Assemble team
  - Educate employees
  - Educate management/leaders
  - Perform assessments
    - Info tracking within the entity
    - Info tracking outside the entity (Business Associates)
  - Prepare policies, procedures and documents.

Team Assembly

- Multiple teams?
  - Corporate vs. Acute vs. Non-acute vs. Research.
- Department heads?
  - How low do you go?
- CEO?
- Possible members: IT manager, manager of health information, director of admissions, risk manager, compliance officer, vendor contracting manager, provider relations manager or chief of medical staff, IRB chairman, business office, legal.

Team building

- BUILD the team.
  - High profile.
  - Educate, educate, educate.
  - Lay out responsibilities up front.
  - Privacy Officer explains goals and timelines.
  - Executives support team.

Now what?

- We have a high profile, executive-supported, educated team that knows its responsibilities, goals and timelines. Now what does the team do?

Assessments

- Think like a compliance plan.
- Analyze ALL individually identifiable health information:
  - Who sees what information at what times and where within the entity for what purposes?
  - Same for outside of the entity.
  - Diagram or map all this.

“Inside” the Entity

- Department self-assessments.
- Specifically examine: transcriptionists, E-web coding, nurses (charts, computer monitors, nurses statements), volunteers, business office.
- Special rules: behavioral health, research, marketing, fundraising.
- Make and post a flow chart for all information.

Outside the Entity

- Have each department list contracts/relationships.
  - Surveys, interviews
  - ID who needs what information
- Pay attention to collection companies, outside auditors, cancer registry.
- Include legal, consulting, data aggregation and financial services.
- Limit to those identified as “business associates.”

Keep in mind

- Who really needs what information?
- Who has access but does not need the information.

Plan Formation

- Use the assessment to formulate a Privacy Plan and/or Policy.
- Categorize all assessed information into routine disclosures and non-routine disclosures.
  - Sub-categorize by type of information and/or department
- Create a standardized protocol for each routine type of disclosure.
- Create a standardized protocol for reviewing various types of non-routine disclosures.

Plan adoption

- First, get department heads' approval.
- Second, get CEO's approval.
- Finally, get formal approval from the Board.

Plan Implementation

- Training on protocols in plan.
- Posting/disseminating the plan to employees.
- Testing.
- Routine training for new employees.
- Communication mechanism.

Documents

- Prepare notice, consent, authorization, model business associate language.
- Train applicable employees on use.
- Determine activities for which authorizations will be needed on a recurring basis.

Patient rights

- Create a system to:
  - Document what individually identifiable health information goes where.
  - Create protocol on the right to inspect, copy and revoke consent, as well as grounds for denial and due process review.
  - Flag when authorizations are necessary.

Business Associates

- Amend or prepare contracts.
- Make sure safeguards are instituted.
- Form a business associate policy.

Minimum Necessary

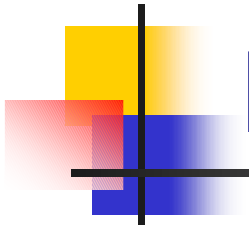
- Form a specific protocol on how to reveal only minimum necessary information.
  - By department.
  - By type of document/information.
  - By job title.

De-identification & Opt-out

- Form a specific protocol on who, how, when and what to de-identify information.
- Form a specific protocol relating to when patients can opt-in/out for directory or marketing (hospital).

Post Implementation

- Privately test employees
- Periodic audits and education
- Identify gaps and report to employees
- Document on-going efforts (drafts, ideas)
- Conduct investigations promptly and respond appropriately



Deadline!

April 14, 2003

Questions

Ann M. Bittinger, Esq.

Kutak Rock, LLP

200 Valencia Place

444 W. 47th Street

Kansas City, MO 64112-1914

ann.bittinger@kutakrock.com

(816) 960-0090