6.02 Advanced Issues in Privacy: Developing Workable Policies and Procedures – Assuring they are a Shield Versus a Sword

Leslie C. Bender

General Counsel & Privacy Officer

roiWebEd Company

www.roiWebEd.com

Guidance given in this presentation is not intended as legal advice. An organization is encouraged to obtain the advice of its own legal counsel, familiar with the organization's unique circumstances and relevant state laws. Information is these materials is accurate as of the date of this presentation; however, please note that caselaw, statutes and regulations may change over time.

Workable

Workable – *adj.* 1. Capable of being worked.
2. Practicable or feasible.

Policy

Policy – *n.* 1. A method or course of action adopted by a government, business organization, etc., designed to influence and determine decisions. 2. A guiding principle or procedure.

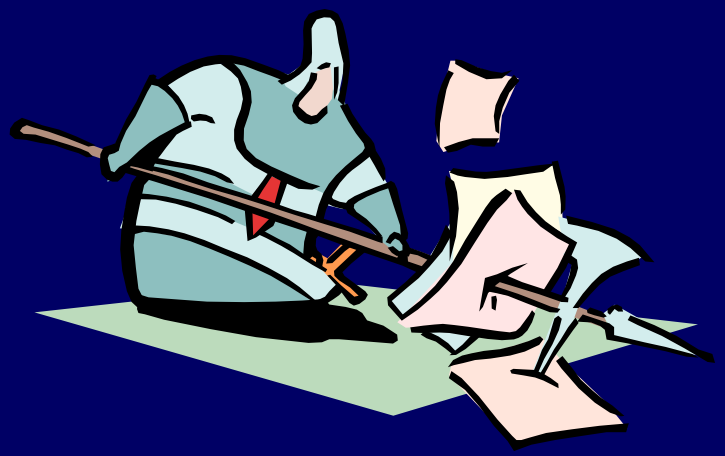
Procedure

Procedure – *n*. 1. A manner of proceeding. 2. A series of steps or course of action. 3. A set of established forms for conducting business or public affairs.

Agenda

1. Privacy Rule guidance on policies and procedures
2. Risks associated with privacy policy and procedure problems
   - Reputational damage
   - Private lawsuits, consumer protection actions
   - Action by other regulatory bodies
   - HHS enforcement
3. Recommendations

What guidance does HIPAA's Privacy Rule provide in regard to policies and procedures?



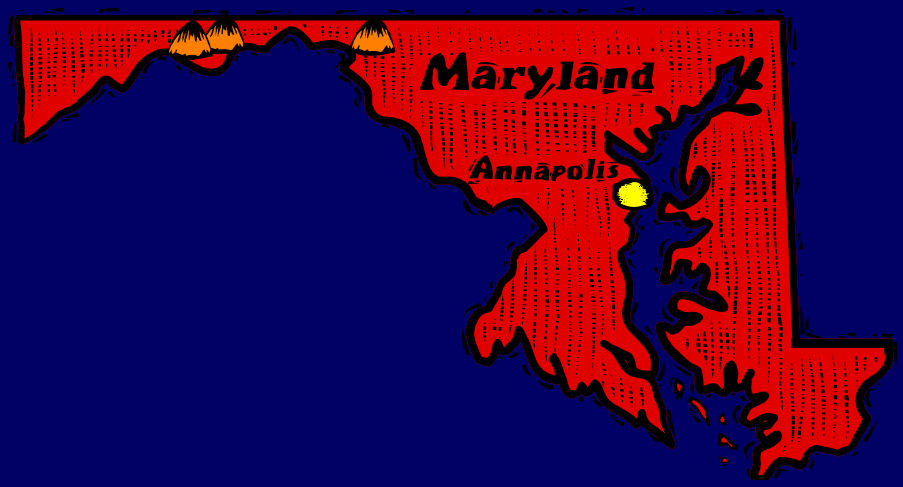
Administrative requirements found in the Privacy Rule include standards and implementation specifications that map a course for compliance

See, 45 CFR Section 164.530

P&P Map in HIPAA

The regulatory guidance offered in the Privacy Rule maps "minimal compliance" standards and specifications, per HHS.

Covered entities are to scale the Privacy Rule's standards and specifications to fit their unique circumstances.



What's charted on the map -

1. Accountability
2. Expectation setting through documentation of policies and procedures
3. Avenues for operationalizing the policies and procedures
4. Meaningful opportunities for individuals to help police covered entities' compliance with their own policies and procedures

Policy & Procedure Accountability

- Personnel designation – privacy official and contact person responsible for developing and implementing a covered entity's policies and procedures
- Consequences for violating policies and procedures – a covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the [Privacy Rule]
- Mitigation – a covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of the [Privacy Rule]

Expectation setting and documentation

Development and implementation of written policies and procedures (and related documentation) with respect to protected health information that are designed to comply with the standards, implementation specifications or other requirements of the Privacy Rule

Avenues for operationalizing the policies and procedures

- Safeguards – administrative, technical, and physical safeguards to protect the privacy of protected health information "from any intentional or unintentional use or disclosure that is in violation of [the Privacy Rule]"
- Training – of all members of workforce on the policies and procedures with respect to protected health information "as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity"

Protection for individuals' expectations about privacy

- Notice of privacy practices – a means for informing individuals about their privacy rights to allow them the opportunity to make informed decisions
- Complaints – provide a process for individuals to make complaints concerning the covered entity's policies and procedures … or its compliance with such policies or procedures or the requirements of the [Privacy Rule]
- Refraining from retaliatory or intimidating acts that would inhibit, discourage, or otherwise interfere with individuals' freedom to exercise HIPAA rights or complain about suspected HIPAA violations
- Refraining from requiring individuals to waive HIPAA rights

Policies & Procedures

The policies and procedures a covered entity must implement

- Should be designed to comply with the Privacy Rule
- Must be designed so as to take into account the size and type of activities that relate to PHI undertaken by the covered entity to ensure compliance with the Privacy Rule
- May not permit or excuse an action that violates any other standard or implementation specification in the Privacy Rule

Continuous improvement, monitoring

The Privacy Rule mandates that a covered entity change or update its policies and procedures as "necessary and appropriate" to comply with changes in the law – and if in so doing makes a material change in its privacy practices, must modify its notice of privacy practices.

A covered entity may reserve to itself the right to make changes in its notice of privacy practices as circumstances dictate.

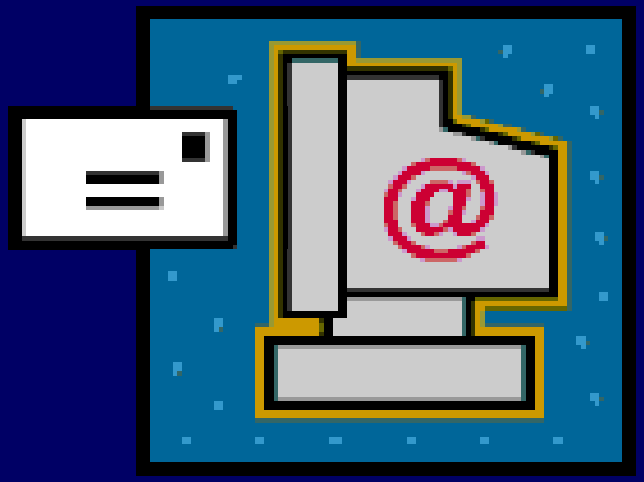
Potential consequences of policy and procedure problems

Case study in privacy policy and procedure problems: Eli Lilly

-Eli Lilly had numerous on and off line privacy promises and policies

-Programmer developing an email to 669 Prozac users and subscribers to medi messenger unaware

-Email message revealed identities of all subscribers to each other



HIPAA and the FTC's Eli Lilly Prescription for Privacy Implementation

- Eli Lilly situation occurred pre-HIPAA
- Eli Lilly suffered reputational damage and did not profit from privacy faux pas
- FTC, after investigation and negotiation, found Eli Lilly's unintentional privacy breach to be an unfair or deceptive trade practice under Section 5 of the FTC Act
- The FTC and Eli Lilly entered into a "consent agreement" with a term of 20 or more years, allowing for regulatory oversight of Eli Lilly's privacy practices – the parameters of which bear a strong resemblance to HIPAA's Privacy Rule

What does the FTC's action in Eli Lilly have to do with HIPAA?

- Eli Lilly is clear regulatory evidence that well drafted privacy programs will be deadly if they are not operationalized
- Privacy promises made to consumers by health care organizations or other businesses entrusted with sensitive health or other information should be made, but must be supported by an infrastructure and series of checks and balances to assure they will not be broken
- Consumers do reveal "non public" information in exchange for important services or benefits out of a belief in the privacy or confidentiality of that information exchange

Lessons learned from Eli Lilly

- It is essential to develop privacy policies and procedures that are accessible to and understood by your workforce
- When developing policies and procedures they should not only meet pure HIPAA legal requirements but should clearly state your organization's position on critical HIPAA issues and provide guidance on how to act or refrain from acting

Policies & Procedures: Scaled to Fit

HIPAA Standard: "The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the [organization], to ensure …compliance."

- What policies and procedures does your organization already have?
- Where can these policies and procedures be found? Where will your workforce look for them?

Policy and Procedure Development - one of several related steps in a HIPAA Compliance Program

Once you have analyzed the requirements of the Privacy Rule and any state laws with which you have to comply, a list or set of gaps should result that will dictate where your organization will need to -

- Define its position or perspective on particular issues pertaining to the collection, use, disclosure, and potential re-disclosure of protected health information
- Describe a means or set of practices for bringing the policy to life, procedures
- Assign responsibility to an individual or group of individuals for carrying out the policy and procedures and from whom further information can be obtained

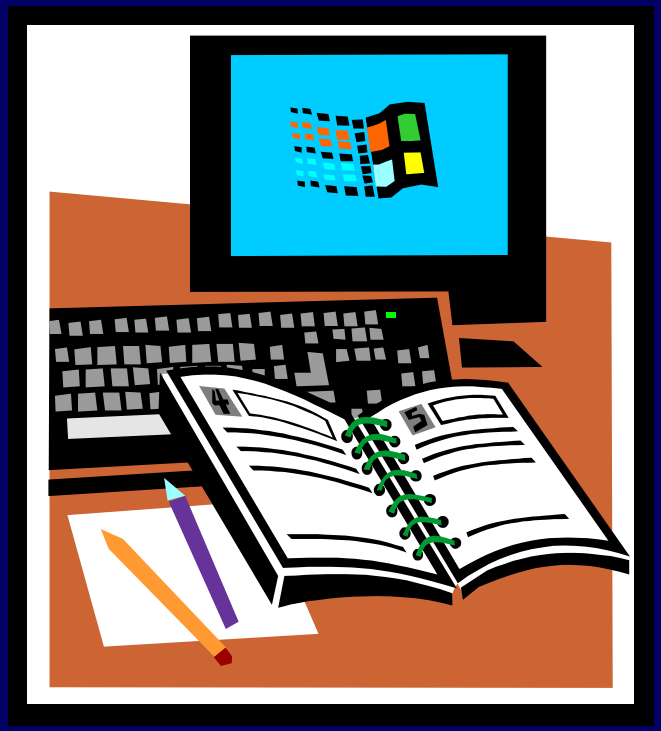
HIPAA Policies and Procedures – Where do they go?

- Evaluate the pros and cons of inserting HIPAA policies and procedures in existing manuals or guides versus developing stand-alone HIPAA compliance guides or manuals
- Form for policies and procedures: paper, electronic, or both? Where are they most likely to be found and read?

Policies and Procedures – Format?

Write policies and procedures in plain language, easy to understand and apply

Sound from legal and operational perspective



Breathing life into policies and procedures: training

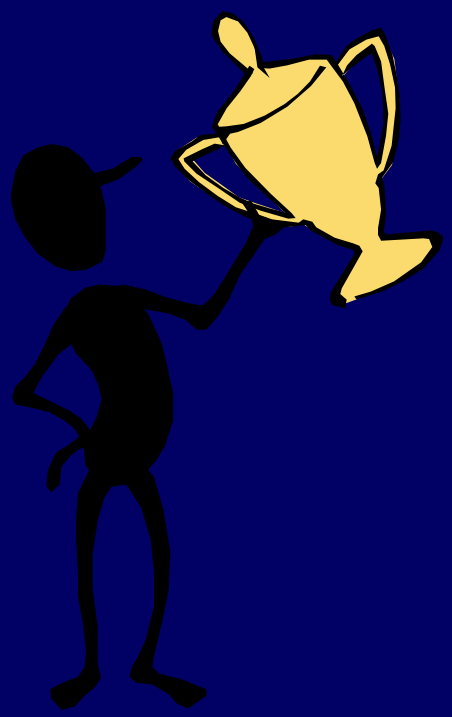
An organization must train all members of its workforce on the policies and procedures with respect to protected health information – by no later than that organization's compliance date (4/14/2003)

- "Workforce" – employees, volunteers, trainees, and "other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity

Continuous improvement and policies and procedures

Training and education approach – regardless of form (e.g., classroom style, team meetings, manuals, web based training) – each approach should be "continuous" with reminders, awareness programs

Performance Criteria; Service Objectives

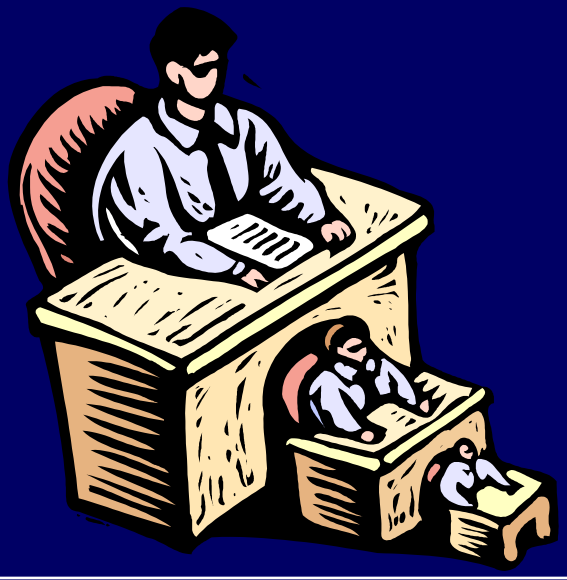


While HIPAA mandates "sanctions" for failing to comply with policies and procedures, will your organization "reward" individuals for excellence in privacy compliance? Will privacy compliance be a factor in performance evaluations?

Monitoring, Assessment, Audit

- Observe program in action
- Adjust to meet changing needs and any legal trends
- Early detection monitoring – are certain policies and procedures difficult to adopt in your corporate culture?
- Update and communicate changes

Complaints



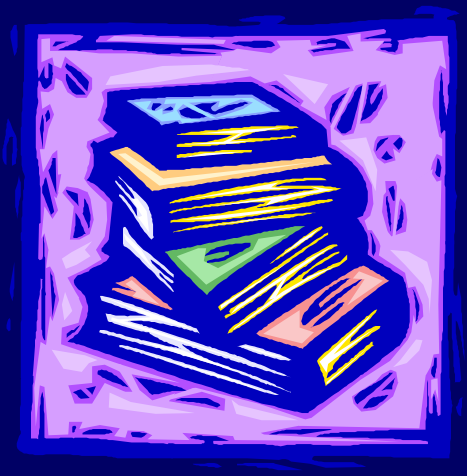
An organization must provide a process that allows individuals to make complaints regarding the organization's privacy policies and procedures – do your processes allow you to truly learn from your mistakes?

Compliance Checklist

- ✓Policies & procedures –
  - ✓ scaled to fit;
  - ✓ written in plain and understandable language
  - ✓ Sound from both a legal and operational perspective
- ✓Privacy official
- ✓Safeguards – technical, administrative, physical
- ✓Implementation Program
- ✓Training
- ✓Continuous Improvement
- ✓Assessment, Audit
- ✓Sanctions
- ✓Complaints
- ✓Documentation
- ✓Mitigate

Where to Get More Information

- HIPAA Privacy Regulations: 45 CFR Section 164.530 and FTC's proposed Consent Agreement in the Eli Lilly Matter
- eBibliography
- Websites of both the Federal Trade Commission and the Department of Health and Human Services
- Look for and subscribe to relevant eAlerts and eNewsletters – iHealthbeat (www.chcf.org)




Thank you.
Comments?
Contact information:
LCB@theROI.com